BUNDESKANZLERAMT

Datenschutzgesetz 1998

Entwurf **GZ 810. 026/8-V/3/98**

Entwurf eines Bundesgesetzes
über den Schutz personenbezogener Daten

Datenschutzgesetz 1998 - DSG

Entwurf

Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 1998[1] - DSG)

Der Nationalrat hat beschlossen:

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 er **selbst** daran ein schutzwürdiges Interesse hat.

(2) Beschränkungen des Rechtes nach Abs. 1 **durch Verwendung personenbezogener Daten** sind nur zur Wahrung **überwiegender** berechtigter Interessen eines anderen oder auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten (BGBl. Nr. 210/1958) genannten Gründen notwendig sind. **Auch im Falle solcher zulässiger Beschränkungen darf nur die jeweils gelindeste zielführende Art des Eingriffs in das Grundrecht gewählt werden.**

(3) Beschränkungen des Rechtes nach Abs. 1 durch Verwendung von Daten natürlicher Personen über rassische und ethnische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben sind unzulässig, soweit sich aus gesetzlichen Vorschriften nicht anderes ergibt. Derartige Vorschriften müssen zur Wahrung wichtiger öffentlicher Interessen notwendig sein und angemessene Garantien vorsehen.

(4) Jedermann hat, soweit **ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuellen Dateien bestimmt sind,** nach Maßgabe gesetzlicher Bestimmungen

1. das Recht auf Auskunft darüber, wer welche Daten über ihn ermittelt oder 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 ermittelter oder verarbeiteter Daten. **Hiebei sind überwiegende schutzwürdige, sich aus der besonderen Situation des Betroffenen ergebende Gründe zu berücksichtigen.**

(5) Beschränkungen der Rechte nach Abs. 4 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

---

[1] Die Jahreszahlen im Titel wurden gegenüber dem versendeten Entwurf geringfügig verändert.

(6) **Gegen** Rechtsträger, **die** in Formen des **Privatrechts eingerichtet sind, ist, soweit sie nicht in Vollziehung der Gesetze tätig werden,** das Grundrecht auf Datenschutz im **Zivilrechtsweg** geltend zu machen. **Für Entscheidungen über die Durchsetzung des Rechts auf Auskunft ist in allen Fällen die Datenschutzkommission zuständig.**

ANWENDUNGSBEREICH

§ 2. (1) Die Bestimmungen dieses Bundesgesetzes sind anzuwenden auf die Verwendung von personenbezogenen Daten im Inland (§ 3 Z 16). Darüber hinaus findet dieses Bundesgesetz auf die Verwendung von Daten in anderen Mitgliedstaaten der Europäischen Union Anwendung, wenn sie für Zwecke einer im Inland gelegenen Niederlassung (§ 3 Z 17) eines Auftraggebers (§ 3 Z 4) erfolgt.

(2) Abweichend von Abs. 1 gilt das Recht des Sitzstaates, wenn ein Auftraggeber (§ 3 Z 4) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union Daten im Inland (§ 3 Z 16) zu einem Zweck verwendet, der keiner Niederlassung (§ 3 Z 17) dieses Auftraggebers im Inland zuzurechnen ist.

(3) Weiters findet dieses Bundesgesetz keine Anwendung, soweit personenbezogene Daten durch österreichisches Hoheitsgebiet nur durchgeführt werden.

Artikel 2

1. Abschnitt

ALLGEMEINES

DEFINITIONEN

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

1. „Daten“: Angaben **über Betroffene (Z 3), deren Identität** bestimmt oder **ohne unverhältnismäßigen Aufwand direkt oder indirekt** bestimmbar **ist** (personenbezogene Daten);
2. „**sensible Daten“: Daten über rassische und ethnische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugungen, Gesundheit oder Sexualleben von natürlichen Personen (besonders schutzwürdige Daten);**
3. „Betroffener“: Jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder mit Rechten und Pflichten ausgestattete Personengemeinschaft, deren Daten verwendet (Z 14) werden;
4. „Auftraggeber“: jede natürliche oder juristische Person oder mit Rechten und Pflichten ausgestattete Personengemeinschaft oder jedes Organ einer Gebietskörperschaft, von dem **allein oder gemeinsam mit anderen die Entscheidung getroffen wird, Daten für einen bestimmten Zweck zu verwenden (Z 14), wobei die automationsunterstützte Verarbeitung [oder die Verarbeitung in einer manuellen Datei] (Z 7) vom Auftraggeber entweder selbst durchgeführt wird oder einem Dienstleister (Z 5) zumindest gestattet wird (Verantwortlicher für die Datenverarbeitung).**

5. „Dienstleister“: jede natürliche oder juristische Person oder mit Rechten und Pflichten ausgestattete Personengemeinschaft oder jedes Organ einer Gebietskörperschaft, von dem Daten **im Rahmen des vom Auftraggeber vorgegebenen Zwecks verwendet werden, wobei die automationsunterstützte Verarbeitung [oder die Verarbeitung in einer manuellen Datei] (Z 7) mit dem Auftraggeber entweder ausdrücklich vereinbart oder von ihm zumindest gestattet wurde (Auftragsverarbeiter**);
6. „**Datei“: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium systematisch geordnet ist.**
7. „Datenverarbeitung“: **die Summe der in ihrem Ablauf logisch verbundenen Datenverwendungsschritten**, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (**des Zweckes der Datenverarbeitung**) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen **(automationsunterstützte Datenverarbeitung); [als Datenverarbeitung gilt weiters auch jede nicht automationsunterstützt geführte Datensammlung, wenn sie strukturiert ist und nach mindestens einem Suchkriterium systematisch geordnet ist (manuelle Datei)].**
8. „Ermitteln von Daten“: das Erheben oder sonstige Beschaffen von Daten **im Rahmen einer** Datenverarbeitung;
9. „Verarbeiten von Daten“: das Erfassen, Speichern, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Löschen **oder jede andere Art der Handhabung von Daten einer Datenverarbeitung durch den Auftraggeber oder Dienstleister, soweit es sich nicht um das Überlassen (Z 11) oder Übermitteln (Z 12) oder um die Weitergabe von Daten an den Betroffenen handelt**;
10. „Löschen von Daten“:
    a) das Unkenntlichmachen von Daten in der Weise, daß eine Rekonstruktion nicht möglich ist (physisches Löschen, **Vernichten**);
    b) die Verhinderung des Zugriffs auf Daten durch programmtechnische Maßnahmen (logisches Löschen, **Sperren**);
11. „Überlassen von Daten“: die Weitergabe von Daten **einer Datenverarbeitung** zwischen Auftraggeber und Dienstleister oder zwischen Dienstleistern;
12. „Übermitteln von Daten“: die Weitergabe von Daten **im Rahmen oder** aus einer Datenverarbeitung 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. „**Datenverkehr“: das Übermitteln oder Überlassen von Daten;**
14. **„Verwenden von Daten“: das Ermitteln, Verarbeiten, Übermitteln, oder Überlassen von Daten sowie das Mitteilen von Daten an den Betroffenen;**
15. **„Zustimmung“: die gültige, also insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;**
16. **„Inland“: das österreichische Staatsgebiet sowie jene Orte außerhalb Österreichs, an welchen gemäß Völkerrecht die österreichische Rechtsordnung anzuwenden ist;**
17. **„Niederlassung“: eine durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die tatsächlich Tätigkeiten ausübt.**

ÖFFENTLICHER UND PRIVATER BEREICH

§ 4. (1) Datenverarbeitungen sind dem öffentlichen Bereich im Sinne dieses Gesetzes 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 eines Rechtsträgers des öffentlichen Rechts, oder
2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

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

2. Abschnitt

ZULÄSSIGKEIT DER VERWENDUNG VON DATEN

GRUNDSÄTZE ÜBER DIE DATENQUALITÄT

§ 5. (1) Daten sollen nur

1. **auf rechtmäßige Weise und so, wie es der Übung des redlichen Verkehrs entspricht, verwendet werden;**
2. **für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden;**
3. **soweit sie für den Zweck der Datenverwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;**
4. **so verwendet werden, daß sie 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.**

(2) Daten, die zulässigerweise veröffentlicht wurden und allgemein zugänglich sind, dürfen für Zwecke, die mit dem Veröffentlichungszweck nicht unvereinbar sind, von jedermann verwendet werden. Bei sensiblen Daten gilt dies nur dann, wenn die Daten offenkundig vom Betroffenen selbst öffentlich gemacht wurden.

(3) Der Auftraggeber trägt bei seinen Datenverarbeitungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt auch dann, wenn er für die Datenverarbeitung Dienstleister heranzieht.

(4) Der Auftraggeber einer diesem Bundesgesetz unterliegenden Datenverarbeitung 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.

(5) Zur näheren Festlegung dessen, was in einzelnen Bereichen der Datenverwendung als Übung des redlichen Verkehrs angesehen werden kann, können Berufsverbände und vergleichbare Einrichtungen Verhaltensregeln ausarbeiten, die vor ihrer Veröffentlichung dem Bundeskanzleramt zur Begutachtung ihrer Übereinstimmung mit den Bestimmungen dieses Bundesgesetzes vorzulegen sind.

BESONDERE BESTIMMUNGEN FÜR DIE ZULÄSSIGKEIT DER ERMITTLUNG UND VERARBEITUNG VON DATEN

§ 6. (1) Für eine Datenverarbeitung dürfen Daten unter Einhaltung der Grundsätze des § 5 ermittelt und verarbeitet werden, wenn hiefür eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung besteht.

(2) Darüber hinaus dürfen Daten unter Einhaltung der Grundsätze des § 5 Abs. 1 und 2 dann ermittelt und verarbeitet werden, wenn

1. **die Datenverarbeitung für die Verwirklichung des berechtigten Zwecks des Auftraggebers erforderlich ist und**
2. **durch die Datenverarbeitung überwiegende schutzwürdige Geheimhaltungsinteressen des Betroffenen, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, nicht verletzt werden; bei sensiblen Daten gilt, daß ihre Verwendung immer überwiegende schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt, es sei denn, daß sich die Zulässigkeit ihrer Verwendung aus gesetzlichen Vorschriften, wie insbesondere aus Abs. 4 oder aus § 41, ergibt.**

(3) Bei einem Auftraggeber des öffentlichen Bereichs, der in Vollziehung der Gesetze tätig wird, ist eine Datenverarbeitung dann für die Verwirklichung seines berechtigten Zwecks (Abs. 2 Z 1) erforderlich, wenn die Datenverarbeitung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe eine wesentliche Voraussetzung bildet.

(4) Überwiegende schutzwürdige Geheimhaltungsinteressen des Betroffenen im Sinne des Abs. 2 Z 2 sind insbesondere dann nicht verletzt, wenn

1. **der Betroffene der Ermittlung oder Verarbeitung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt; im Falle der Ermittlung oder Verarbeitung sensibler Daten muß die Zustimmung ausdrücklich gegeben worden sein;**
2. **die Ermittlung oder Verarbeitung zur Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist und eine der Z 1 entsprechende Zustimmung nicht rechtzeitig eingeholt werden konnte;**
3. **die Ermittlung oder Verarbeitung von nicht sensiblen Daten zur Wahrung lebenswichtiger Interessen eines anderen Menschen notwendig ist;**
4. **Daten ermittelt oder verarbeitet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben.**

(5) Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten dann ermitteln und verarbeiten, wenn sie ihnen vom Betroffenen[2] selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise, insbesondere in Übereinstimmung mit § 7, zugekommen sind.

BESONDERE BESTIMMUNGEN FÜR DIE ZULÄSSIGKEIT DER ÜBERMITTLUNG VON DATEN

§ 7. (1) Unter Einhaltung der Grundsätze des § 5 Abs. 1 und 2 dürfen Auftraggeber an Empfänger, die einen ausreichenden berechtigten Zweck glaubhaft gemacht haben,

---

[2] Im versendeten Entwurf stand irrtümlich „Auftraggeber“.

zulässigerweise ermittelte oder verarbeitete Daten unter folgenden Voraussetzungen übermitteln:

1. **wenn hiefür eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung besteht;**
2. **wenn der Betroffene seine Zustimmung zur Übermittlung gegeben hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit künftiger Übermittlungen bewirkt; bei sensiblen Daten muß die Zustimmung ausdrücklich erteilt worden sein;**
3. **wenn die Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist und eine Z 2 entsprechende Zustimmung des Betroffenen nicht rechtzeitig eingeholt werden konnte;**
4. **wenn an der Übermittlung ein das schutzwürdige Geheimhaltungsinteresse des Betroffenen überwiegendes berechtigtes Interesse des Auftraggebers oder eines Dritten besteht. Die Übermittlung sensibler Daten ist jedoch nur dann zulässig, wenn sich dies aus besonderen Rechtsvorschriften, wie insbesondere § 41, ergibt.**

(2) Abs. 1 gilt für Übermittlungen aus Datenverarbeitungen, die von Auftraggebern des öffentlichen Bereichs in Vollziehung der Gesetze vorgenommen werden, mit folgender Maßgabe:

1. **Ein überwiegendes berechtigtes Interesse (Abs. 1 Z 4) an der Übermittlung ist insbesondere dann gegeben, wenn die Übermittlung in Erfüllung der Verpflichtung zur Amtshilfe geschieht;**
2. **sofern on-line Übermittlungen nicht gesetzlich ausdrücklich vorgesehen sind, dürfen sie nur bei Übermittlungen gemäß Abs. 1 Z 1 oder 2 vorgenommen werden.**

(3) Bestehende gesetzliche Verschwiegenheitspflichten werden durch Abs. 1 und 2 nicht berührt.

(4) Daten, die eine natürliche Personen gemäß § 6 Abs. 5 für ausschließlich persönliche oder familiäre Tätigkeiten ermittelt oder verarbeitet, dürfen für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.

(5) Nicht registrierte Übermittlungen sind so zu protokollieren, daß dem Betroffenen Auskunft gemäß § 23 gegeben werden kann. In der Standardverordnung (§ 15 Abs. 4 Z 4) und in der Musterverordnung (§ 16 Abs. 2) vorgesehene Übermittlungen bedürfen keiner Protokollierung.

ZULÄSSIGKEIT DER ÜBERLASSUNG VON DATEN ZUR ERBRINGUNG VON DIENSTLEISTUNGEN

§ 8. (1) Soweit Auftraggeber nach § 6 zur Ermittlung und Verarbeitung von Daten berechtigt sind, dürfen sie bei ihren Datenverarbeitungen Dienstleister in Anspruch nehmen, **wenn diese hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat sich von der Einhaltung der notwendigen Maßnahmen beim Dienstleister zu überzeugen.**

(2) Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs 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 gelten die Bestimmungen des **§ 26 Abs. 3 Z 4.**

PFLICHTEN DES DIENSTLEISTERS

§ 9. (1) Dienstleister haben bei der Verwendung von Daten für den Auftraggeber 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 § 12 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber gemäß § 13 zur Geheimhaltung von Daten 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 nachvollziehbar festzuhalten.

GENEHMIGUNGSFREIE ÜBERMITTLUNG UND ÜBERLASSUNG VON DATEN IN DAS AUSLAND

§ 10. (1) Die Übermittlung von Daten an Empfänger in Mitgliedstaaten der Europäischen Union ist keinen Beschränkungen im Sinne des § 11 unterworfen, soweit Daten natürlicher Personen weitergegeben werden und der Zweck des Datenverkehrs eine Angelegenheit des Gemeinschaftsrechts betrifft. Die Datenüberlassung in einen Mitgliedstaat der Europäischen Union zwecks Dienstleistungsverarbeitung ist jedenfalls ohne Genehmigung im Sinne des § 11 zulässig.

(2) Keiner Genehmigung gemäß § 11 bedarf weiters der Datenverkehr mit Empfängern in Drittstaaten mit angemessenem Datenschutzniveau. Welche Drittstaaten und welche Mitgliedstaaten der Europäischen Union in den von Abs. 1 nicht erfaßten Fällen ein angemessenes Datenschutzniveau gewährleisten, wird unter Beachtung des § 51 durch Verordnung des Bundeskanzlers festgestellt. Maßgebend für die Angemessenheit des Schutzniveaus ist die Ausgestaltung der Grundsätze des § 5 Abs. 1 in der ausländischen Rechtsordnung und das Vorhandensein wirksamer Garantien für ihre Durchsetzung.

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

1. **die Übermittlung (Überlassung) in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder**
2. **der Betroffene seine Zustimmung zur Übermittlung (Überlassung) seiner Daten ins Ausland gegeben hat, was insbesondere auch dann vorliegt, wenn die Übermittlung (Überlassung) die notwendige Folge einer vom Betroffenen in voller Kenntnis der Sachlage veranlaßten Handlung des Auftraggebers darstellt oder**
3. **die Daten im Inland zulässigerweise veröffentlicht wurden, insbesondere in einem zur Information der Öffentlichkeit bestimmten Register, wobei dann, wenn für die Einsicht ein berechtigtes Interesse gefordert ist, dieses auch beim Empfänger der Übermittlung im Ausland gegeben sein muß, oder**
4. **ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener gültiger Vertrag nicht anders als durch Übermittlung (Überlassung) der Daten erfüllt werden kann oder**
5. **die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor den zuständigen ausländischen Behörden erforderlich ist und dem Auftraggeber rechtmäßig zugekommene Daten betrifft, oder**
6. **es sich um Übermittlungen oder Überlassungen handelt, die in einer Standardverordnung (§ 15 Abs. 4 Z 4) ausdrücklich angeführt sind.**

(4) Wenn eine Übermittlung oder Überlassung von Daten ins Ausland

1. **zur Wahrung eines wichtigen öffentlichen Interesses oder**
2. **zur Wahrung eines lebenswichtigen Interesses eines Menschenso dringlich ist, daß eine Genehmigung der Datenschutzkommission gemäß § 11 nicht eingeholt werden kann, ohne die genannten Interessen wesentlich zu gefährden, darf sie ohne Genehmigung vorgenommen werden, muß aber der Datenschutzkommission umgehend nachträglich mitgeteilt werden.**

(5) Voraussetzung für die Zulässigkeit von genehmigungsfreien Übermittlungen und Überlassungen gemäß Abs. 1 bis 4 in das Ausland ist die Einhaltung der §§ 6 und 7. Bei Überlassungen ins Ausland muß darüberhinaus die schriftliche Zusage des ausländischen Dienstleisters an den inländischen Auftraggeber - oder in den Fällen des § 11 Abs. 4 gegenüber dem inländischen Dienstleister - vorliegen, daß er § 9 Abs. 1 einhalten werde.

GENEHMIGUNGSPFLICHTIGE ÜBERMITTLUNG UND ÜBERLASSUNG VON DATEN INS AUSLAND

§ 11. (1) In den nicht dem § 10 unterliegenden Fällen hat der Auftraggeber zwecks Wahrung des öffentlichen Interesses an der Hintanhaltung von Datenschutzverletzungen durch den Datenverkehr mit dem Ausland vor der Übermittlung oder der Überlassung von Daten in das Ausland eine Genehmigung der Datenschutzkommission einzuholen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen binden wie insbesonders auch an das Vorliegen vertraglicher Zusicherungen des Empfängers an den Antragsteller über die näheren Umstände der Datenverwendung im Ausland.

(2) Die Genehmigung ist unter Beachtung der gemäß § 51 ergangenen Kundmachungen zu erteilen, wenn die Voraussetzungen des § 10 Abs. 5 vorliegen und wenn

1. **für die im Genehmigungsantrag dargestellte Übermittlung oder Überlassung im Empfängerstaat angemessener Datenschutz besteht, was unter Berücksichtigung aller Umstände zu beurteilen ist, 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, die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort geltenden Standesregeln und Sicherheitsstandards; oder**
2. **der Auftraggeber gewährleistet, daß die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen ausreichend gewahrt werden, und dieser Schutz durchsetzbar ist.**

(3) Die Datenschutzkommission hat eine Ausfertigung jedes Bescheides, mit dem eine Übermittlung oder Überlassung von Daten in das Ausland genehmigt wurde, zum Registrierungsakt zu nehmen; die Erteilung einer Genehmigung ist im Datenverarbeitungsregister anzumerken, es sei denn, daß gemäß § 15 Abs. 5 eine Eintragung der Datenverarbeitung in das Datenverarbeitungsregister nicht vorzunehmen war.

(4) 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 Datenverarbeitungen die dem Dienstleister genehmigte Überlassung erfolgen soll; dies ist im Register anzumerken.

DATENSICHERHEITSMASSNAHMEN

§ 12. (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, nach Umfang und Zweck der Verwendung und unter Bedachtnahme auf den Stand der technischen Möglichkeiten sowie auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die **Daten vor unbeabsichtigter Zerstörung und Verlust geschützt sind, ihre** Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht **zugänglich sind und insbesondere von diesen nicht verändert werden können**.

(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 Verarbeitungsvorgänge wie insbesondere Abfragen und Änderungen nachvollzogen werden können,**
8. **eine Dokumentation über die nach Z. 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.**

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

(4) Protokoll- und Dokumentationsdaten dürfen für keine anderen als die in Abs. 2 Z 7 und 8 genannten Zwecke verwendet werden. Sofern gesetzlich nicht ausdrücklich anderes vorgesehen ist, sind diese Daten fünf Jahre lang aufzubewahren.

(5) Für Datenverarbeitungen, die auf Grund ihrer besonderen Eignung, in die schutzwürdigen Geheimhaltungsinteressen der Betroffenen einzugreifen, der Vorabkontrolle gemäß § 15 Abs. 2 unterliegen, hat der Auftraggeber - unbeschadet seiner Verantwortung gegenüber dem Betroffenen - einen Mitarbeiter oder eine andere geeignete Person zu bestellen, die mit der Wahrnehmung der Datensicherheit eigens betraut ist.

DATENGEHEIMNIS

§ 13. (1) Mitarbeiter eines Auftraggebers oder Dienstleisters dürfen Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger **gesetzlicher** Verschwiegenheitspflichten nur auf Grund einer ausdrücklichen Anordnung des Auftraggebers oder Dienstleisters übermitteln (Datengeheimnis).

(2) Auftraggeber und Dienstleister haben, **sofern eine solche Verpflichtung ihrer Mitarbeiter nicht schon kraft Gesetzes besteht**, diese vertraglich zu verpflichten, daß sie Daten aus Datenverarbeitungen nur auf Grund von Anordnungen gemäß Abs. 1 übermitteln und das Datengeheimnis auch nach Beendigung des Mitarbeiterverhältnisses zum Auftraggeber oder Dienstleister einhalten werden.

(3) Die Organe eines Auftraggebers oder Dienstleisters, die gegenüber Mitarbeitern anordnungsbefugt sind, dürfen eine Anordnungen nach Abs. 1 nur erteilen, wenn die dadurch verfügte Übermittlung von Daten nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben ihre Mitarbeiter über die für sie geltenden Übermittlungsanordnungen und über die strafrechtlichen Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Aus der Verweigerung der Ausführung eines Auftrages, der gegen die §§ 5, 7 und 11 verstoßen würde, darf dem Mitarbeiter kein Nachteil erwachsen.

(5) In einem behördlichen Verfahren kann sich niemand seiner Zeugenpflicht unter Berufung auf das Datengeheimnis entschlagen.

3. Abschnitt

PUBLIZITÄT DER DATENVERARBEITUNGEN

DATENVERARBEITUNGSREGISTER

§ 14. (1) Bei der Datenschutzkommission ist ein Register der Datenverarbeitungen zum Zweck der Prüfung der Rechtmäßigkeit von Datenverarbeitungen und zum Zweck der Information der Betroffenen eingerichtet.

(2) Jedermann kann in das Register Einsicht nehmen. In die im Registrierungsakt befindlichen Genehmigungsbescheide der Datenschutzkommission über Datenverkehr ins Ausland ist Einsicht zu gewähren, soweit der Einsichtswerber glaubhaft macht, daß er Betroffener der genehmigten Übermittlung oder Überlassung ist, und soweit nicht überwiegende schutzwürdige Geheimhaltungsinteressen des Auftraggebers - **etwa nach § 15 Abs. 5** - 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 und die Möglichkeit vorzusehen, eine Meldung (§§ 15 und 16) auf automationsunterstütztem Wege vorzunehmen.

MELDEPFLICHT DES AUFTRAGGEBERS

§ 15. (1) Jeder Auftraggeber hat, sofern in Abs. 4 nicht anderes bestimmt ist, vor Aufnahme einer Datenverarbeitung an die Datenschutzkommission eine Meldung mit dem in § 16 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. Die Datenverarbeitung darf - außer in den Fällen des Abs. 2 - unmittelbar nach Abgabe der Meldung aufgenommen werden.

(2) Datenverarbeitungen,die
1. **sensible Daten oder**
2. **die Beurteilung der finanziellen Lage des Betroffenen oder**
3. **strafrechtlich relevante Sachverhalte betreffen oder**
4. **in Form eines Informationsverbundsystems (§ 46) durchgeführt werden sollen,**

dürfen erst nach ihrer Prüfung und der Registrierung durch die Datenschutzkommission aufgenommen werden (Vorabkontrolle).

(3) Die automationsunterstützte Erstellung und Archivierung von nicht strukturierten Texten (Textverarbeitung) gilt, soweit sie in unmittelbarem Zusammenhang mit Dateien steht, als von der Meldung der Datei mitumfaßt.

(4) Keine Meldepflicht besteht für Datenverarbeitungen, die

1. **von natürlichen Personen gemäß § 6 Abs. 5 ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden;**
2. **ausschließlich in der Abfrage von zulässigerweise veröffentlichten Datensammlungen bestehen;**
3. **die Führung von Registern oder Verzeichnissen betreffen, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses;**
4. **Standardverarbeitungen darstellen: Der Bundeskanzler kann durch Verordnung Typen von Datenverarbeitungen und Übermittlungen aus diesen zu Standardverarbeitungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verarbeitungszwecks und der zu verarbeitenden Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardverarbeitung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.**

(5) Beabsichtigte Datenverarbeitungen für Zwecke

1. **des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich,**
2. **der Sicherung der Einsatzbereitschaft des Bundesheeres oder der umfassenden Landesverteidigung oder**
3. **der Strafrechtspflege**

sind, außer bei Gefahr im Verzug, der Datenschutzkommission zu melden. Stellt der Auftraggeber den Antrag, daß angesichts des Inhalts der Datenverarbeitung die Eintragung in das öffentlich einsehbare Register unterbleiben solle, so entscheidet die Datenschutzkommission über diesen Antrag mit Bescheid.

NOTWENDIGER INHALT DER MELDUNG

§ 16. (1) Eine Meldung im Sinne des § 15 hat zu enthalten:

1. **den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 5 Abs. 4; weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde;**
2. **den Nachweis von Rechtsgrundlagen für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist;**
3. **den Zweck und die Rechtsgrundlagen für die zu registrierende Datenverarbeitung;**
4. **die Kreise der von der Datenverarbeitung Betroffenen und die über sie verarbeiteten Datenarten;**
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;**
6. **soweit eine Genehmigung für den internationalen Datenverkehr gemäß § 11 einzuholen war - die Geschäftszahl der Genehmigung der Datenschutzkommission;**
7. **allgemeine Angaben über das Bestehen von Datensicherheitsmaßnahmen im Sinne des § 12, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.**

(2) Wenn eine größere Anzahl von Auftraggebern des öffentlichen Bereichs die gleiche Datenverarbeitung vorzunehmen hat und die Voraussetzungen für die Erklärung zur Standardverarbeitung nicht vorliegen, kann der Bundeskanzler durch Verordnung eine

Mustermeldung verbindlich festlegen. Meldungen über Datenverarbeitungen, die inhaltlich einer Mustermeldung entsprechen, haben folgendes zu enthalten:

1. **die Bezeichnung und Anschrift des Auftraggebers sowie den Nachweis der Rechtsgrundlagen seiner Tätigkeit, soweit dies erforderlich ist;**
2. **die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde;**
3. **die Bezeichnung der Datenverarbeitung gemäß der Musterverordnung.**

(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 Datenverarbeitung ihre schutzwürdigen Geheimhaltungsinteressen verletzt sein könnten. Unstimmigkeit liegt insbesondere auch dann vor, wenn der Inhalt einer gemeldeten Datenverarbeitung durch die gemeldeten Rechtsgrundlagen nicht gedeckt ist.

VERBESSERUNGSVERFAHREN

§ 17. (1) Kommt die Datenschutzkommission bei der Prüfung, der sie alle Meldungen zu unterziehen hat, zur Auffassung, daß eine Meldung mangelhaft im Sinne des § 16 Abs. 3 ist, so ist dem Auftraggeber längstens innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung des Mangels unter Setzung einer Frist aufzutragen.

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

(3) Liegt im Falle des Abs. 1 wegen wesentlicher Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen durch die gemeldete Datenverarbeitung Gefahr im Verzug vor, so hat die Datenschutzkommission die Aufnahme bzw. die Weiterführung der Datenverarbeitung mit Bescheid gemäß § 57 Abs. 1 AVG vorläufig zu untersagen.

REGISTRIERUNG

§ 18. (1) Meldungen gemäß § 16 sind in das Datenverarbeitungsregister einzutragen, wenn

1. **nicht innerhalb von zwei Monaten nach Einlangen der Meldung bei der Datenschutzkommission ein Verbesserungsverfahren gemäß § 17 Abs. 1 eingeleitet wurde;**
2. **der Auftraggeber die verlangten Verbesserungen fristgerecht vorgenommen hat oder**
3. **das Prüfverfahren die Zulässigkeit der Registrierung ergeben hat.**

(2) Dem Auftraggeber ist die Durchführung der Registrierung schriftlich in Form eines Registerauszuges mitzuteilen. Die Mitteilung hat bei der erstmaligen Meldung eines Auftraggebers auch die dem Auftraggeber zugeteilte Registernummer zu enthalten.

RICHTIGSTELLUNG DES REGISTERS

§ 19. (1) Streichungen und Änderungen sind im Datenverarbeitungsregister auf Antrag des Eingetragenen oder in den Fällen der Abs. 2 und 4 von Amts wegen durchzuführen.

(2) Änderungen in der Bezeichnung oder der Anschrift des Auftraggebers sind, sofern sie der Datenschutzkommission aus amtlichen Verlautbarungen zur Kenntnis gelangen, von Amts wegen zu berichtigen. Desgleichen ist von Amts wegen die Streichung aus dem Register vorzunehmen, wenn sich aus einer amtlichen Verlautbarung der Wegfall der Rechtsgrundlage des Auftraggebers ergibt.

(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 oder der Verletzung der Registrierungspflicht begründen, so hat die Datenschutzkommission ein Verfahren zur Feststellung des für die Erfüllung der Registrierungspflicht erheblichen Sachverhalts einzuleiten und das Datenverarbeitungsregister entsprechend dem Ergebnis des Verfahrens zu berichtigen.

PFLICHT ZUR OFFENLEGUNG NICHT MELDEPFLICHTIGER DATENVERARBEITUNGEN

§ 20. Auftraggeber von Standardverarbeitungen haben jedermann auf Antrag darüber Auskunft zu geben, für welche Zwecke sie Standardverarbeitungen durchführen und welche Datenarten, Betroffenenkreise und Empfängerkreise die vorgenommenen Standardverarbeitungen umfassen.

INFORMATIONSPFLICHT DES AUFTRAGGEBERS

§ 21. (1) Der Auftraggeber einer Datenverarbeitung hat bei der erstmaligen Ermittlung von Daten beim Betroffenen diesen über

1. **den Zweck der Datenverarbeitung, für die die Daten erhoben werden, und**
2. **Namen, Adresse und allfällige Registernummer des Auftraggebers**

in geeigneter Weise zu informieren, falls diese Informationen dem Betroffenen im Zeitpunkt der Erhebung nicht bereits in geeigneter Form vorliegen.

(2) Werden Daten für eine Datenverarbeitung nicht beim Betroffenen selbst erhoben, darf die Information über die Identität des Auftraggebers und den Zweck der Datenverwendung entfallen, wenn

1. **diese Informationen dem Betroffenen bereits vorliegen oder**
2. **die Datenverwendung durch Gesetz oder Verordnung ausdrücklich vorgesehen ist oder**
3. **die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder**

4. wenn sie angesichts der verwendeten Datenarten und des Verwendungszwecks einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Der Bundeskanzler kann durch Verordnung für bestimmte Arten von Datenverarbeitungen feststellen, daß die Informationspflicht wegen unverhältnismäßigen Aufwandes entfällt.

(3) Darüber hinausgehende Informationen über die Datenverarbeitung und über eine allfällige Verpflichtung zur Mitwirkung an der Datenermittlung sind zu geben, wenn dies nach der Übung des redlichen Verkehrs erforderlich ist, insbesondere weil wesentliche Abweichungen von der angesichts des Verarbeitungszwecks zu erwartenden Datenverwendung geplant sind.

(4) Die Informationspflicht entfällt, wenn Daten für Zwecke einer Datenverarbeitung ermittelt werden, die gemäß § 15 Abs. 4 und 5 nicht zu melden oder nicht in das Datenverarbeitungsregister einzutragen sind.

PFLICHT ZUR OFFENLEGUNG DER IDENTITÄT DES AUFTRAGGEBERS

§ 22. (1) Bei Übermittlungen und Mitteilungen an Betroffene hat der Auftraggeber seine Identität in einer Weise offenzulegen, die den Betroffenen die Verfolgung ihrer Rechte ermöglicht. Bei meldepflichtigen Datenverarbeitungen ist in Mitteilungen an Betroffene die Registernummer des Auftraggebers anzuführen.

(2) Werden Daten aus einer Datenverarbeitung 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 Datenverarbeitung die Daten stammen. Handelt es sich hiebei um eine meldepflichtige Datenverarbeitung, ist die Registernummer des Auftraggebers beizufügen.

4. Abschnitt

DIE RECHTE DES BETROFFENEN

AUSKUNFTSRECHT

§ 23. (1) Der Auftraggeber hat dem Betroffenen Auskunft über die über ihn ermittelten und 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 in allgemein verständlicher Form die verarbeiteten Daten, ihre Herkunft, allfällige Empfänger, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür anzuführen. Wird zur Verarbeitung ein Dienstleister herangezogen, sind auch Name und Anschrift des Dienstleisters bekanntzugeben, wenn der Betroffene dies verlangt. 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 überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten oder überwiegende öffentliche Interessen, insbesondere

in Form gesetzlicher Auskunftsbeschränkungen und Verschwiegenheitspflichten, dies erfordern; überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich, der Sicherung der Einsatzbereitschaft des Bundesheeres und der umfassende Landesverteidigung sowie der Strafrechtspflege oder aus der Notwendigkeit der Wahrung wichtiger wirtschaftlicher oder finanzieller Interessen des Staates ergeben.

(3) Der Betroffene hat am Auskunftsverfahren in dem ihm zumutbaren Ausmaß mitzuwirken, um nicht gerechtfertigten, unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

(4) Eine Auskunft ist unentgeltlich zu erteilen, **wenn sie Dateien betrifft, die beim Auftraggeber im direkten Zugriff stehen** und wenn der Auskunftswerber im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. **Für alle anderen Fälle kann ein pauschalierter Kostenersatz von S 200,-- verlangt werden, von dem in begründeten Fällen 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.**

(5) Innerhalb von 4 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 nicht gemäß Abs. 3 am Verfahren mitgewirkt oder den Kostenersatz nicht geleistet hat.

(6) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Auskunftswerber innerhalb eines Zeitraums von vier Monaten, im Falle der Erhebung einer Beschwerde gemäß § 27 Abs. 1 an die Datenschutzkommission bis zum rechtskräftigen Abschluß des Verfahrens, nicht löschen.

RECHT AUF RICHTIGSTELLUNG ODER LÖSCHUNG

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

1. **aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Ermittlung oder Verarbeitung bekannt ist;**
2. **auf begründeten Antrag des Betroffenen.**

Die Unvollständigkeit verwendeter Daten bewirkt nur dann eine Pflicht zur Richtigstellung, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenverarbeitung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für die Zwecke der Datenverarbeitung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten.

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

(3) Wenn aus Gründen der Wirtschaftlichkeit die physische Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind diese Daten bis dahin logisch und sodann physisch zu löschen oder richtigzustellen.

(4) Stellt der Betroffene einen Antrag auf Richtigstellung oder Löschung, ist ihm binnen 12 Wochen nach Einlangen des Antrags beim Auftraggeber schriftlich mitzuteilen, ob eine Löschung oder Richtigstellung vorgenommen wurde oder zu begründen, warum dies nicht geschehen ist.

(5) 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.

(6) Bei der Übermittlung und Benützung von Daten, deren Richtigkeit vom Betroffenen bestritten wurde, und bei denen sich weder die Richtigkeit noch die Unrichtigkeit feststellen ließ, ist über Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. **Die Löschung des Bestreitungsvermerks darf nur mit Zustimmung des Betroffenen oder aufgrund einer Entscheidung des zuständigen Gerichtes oder. der Datenschutzkommission erfolgen.**

(7) 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.

WIDERSPRUCHSRECHT

§ 25. (1) Jeder Betroffene hat das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergibt, Widerspruch zu erheben, sofern die Verwendung nicht gesetzlich zwingend vorgesehen ist. Der Auftraggeber der Datenverwendung hat den Betroffenen bei Vorliegen der besonderen Voraussetzungen binnen 4 Wochen aus seiner Datenverarbeitung zu löschen beziehungsweise eine beeinspruchte Übermittlung zu unterlassen.

(2) Widerspruch gegen eine durch Gesetz nicht zwingend vorgesehene Aufnahme in eine öffentlich zugängliche Datei kann vom Betroffenen jederzeit auch ohne Nachweis der Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen mit dem Anspruch auf Löschung erhoben werden.

5. Abschnitt

RECHTSSCHUTZ

KONTROLLBEFUGNISSE DER DATENSCHUTZKOMMISSION

§ 26. (1) Jedermann kann wegen behaupteter Verletzungen seiner Rechte nach diesem Bundesgesetz oder nach datenschutzrechtlichen Vorschriften eines anderen Mitgliedstaats der Europäischen Union, die gemäß § 2 im Inland Anwendung finden, eine Eingabe an die Datenschutzkommission machen. Jede Eingabe ist von der Datenschutzkommission zu prüfen. Dem Einbringer sind das Ergebnis der Prüfung sowie die allenfalls getroffenen Veranlassungen mitzuteilen.

(2) Die Datenschutzkommission kann jederzeit Einschau in Datenverarbeitungen und die diesbezüglichen Unterlagen begehren und Aufklärung vom Auftraggeber der überprüften Datenverarbeitung verlangen. Zwecks Herstellung des rechtmäßigen Zustandes kann sie Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist.

(3) Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes gegen Vorschriften dieses Bundesgesetzes

1. **ein Verfahren zur Überprüfung der Registrierung gemäß § 19 Abs. 4 einleiten, oder**
2. **die zuständige Behörde zwecks Einleitung eines Strafverfahrens insbesondere gemäß §§ 47 und 48 befassen, oder**
3. **bei schwerwiegenden Verstößen von Auftraggebern des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 28 Abs. 4 erheben, oder**
4. **bei Verstößen von Auftraggebern des öffentlichen Bereichs das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder diesen Empfehlungen zu entsprechen und dies der Datenschutzkommission mitzuteilen oder schriftlich zu begründen, warum den Empfehlungen nicht entsprochen wurde.**

(4) Ist die vermutete Verletzung schutzwürdiger Geheimhaltungsinteressen eines Betroffenen im Inland gemäß § 2 nach der Rechtsordnung eines anderen Mitgliedstaats der Europäischen Union zu beurteilen, so kann die Datenschutzkommission die zuständige ausländische Datenschutzkontrollstelle mit dem Ersuchen um Unterstützung befassen.

(5) Die Datenschutzkommission leistet den Unabhängigen Datenschutzkontrollstellen der anderen Mitgliedstaaten der Europäischen Union über Ersuchen Amtshilfe.

BESCHWERDE AN DIE DATENSCHUTZKOMMISSION

§ 27. (1) **Die Datenschutzkommission erkennt über behauptete Verletzungen des Auskunftsrechts gemäß § 23 auf Antrag des Betroffenen.**

(2) Zur Entscheidung über die behauptete Verletzung anderer Betroffenenrechte nach diesem Gesetz ist die Datenschutzkommission dann zuständig, wenn der Betroffene seine Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs richtet.

(3) Bei Gefahr im Verzug für den Beschwerdeführer kann die Datenschutzkommission **die weitere Verwendung von Daten zur Gänze oder teilweise** untersagen.

(4) Wird in einem vor einer anderen Verwaltungsbehörde durchgeführten Verwaltungsverfahren von einer Partei **nicht offenbar mutwillig** behauptet, in ihren Rechten nach diesem Bundesgesetz verletzt zu sein, so hat die Verwaltungsbehörde, außer bei Gefahr im Verzug, ihr Verfahren bis zur Entscheidung dieser Vorfrage durch die Datenschutzkommission auszusetzen und gleichzeitig die Entscheidung bei der Datenschutzkommission zu beantragen. **Im übrigen gelten die Bestimmungen des § 38 AVG.**

ANRUFUNG DER GERICHTE

§ 28. (1) Ansprüche gegen Auftraggeber des privaten Bereichs wegen Verletzung von Rechten des Betroffenen nach diesem Bundesgesetz sind, **soweit es sich nicht um Ansprüche auf Auskunft gemäß § 23 handelt**, **über welche die Datenschutzkommission gemäß § 27 Abs. 1 entscheidet**, auf dem ordentlichen Rechtsweg 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) Für Klagen nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen des Betroffenen können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Auftraggeber oder der Dienstleister seinen gewöhnlichen Aufenthalt oder Sitz hat.

(4) Die Datenschutzkommission kann in Fällen, in welchen sie schwerwiegende Datenschutzverletzungen durch einen Auftraggeber des privaten Bereichs vermutet, eine Feststellungsklage (§ 228 ZPO) bei dem gemäß Abs. 3 zweiter Satz zuständigen Gericht erheben.

(5) Die Datenschutzkommission **kann**, 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) beitreten.

SCHADENERSATZ

§ 29. (1) Sind Daten entgegen den Bestimmungen dieses Bundesgesetzes verwendet worden, hat der Betroffene Anspruch auf Ersatz des erlittenen Schadens. In besonders schwerwiegenden Fällen, insbesondere bei der rechtswidrigen Verwendung von sensiblen Daten, von Daten über die finanzielle Lage des Betroffenen oder von Daten, die im Zusammenhang mit strafbaren Handlungen stehen, kann der Betroffene eine angemessene Entschädigung für die erlittene Beeinträchtigung, deren Höhe S 200. 000,-- nicht übersteigt, verlangen.

(2) Die Ersatzpflicht nach Abs. 1 trifft den Auftraggeber und den Dienstleister. Diese können teilweise oder ganz von der Haftung befreit werden, wenn sie nachweisen, daß der Umstand, durch den der Schaden eingetreten ist, ihnen und ihren Leuten nicht zur Last gelegt werden kann.

(3) Der Auftraggeber und der Dienstleister haften zur ungeteilten Hand, unabhängig davon, in welchem Bereich das schädigende Ereignis eingetreten ist.

(4) Der Auftraggeber und der Dienstleister haften für das Verschulden ihrer gesetzlichen Vertreter sowie der Personen, deren sie sich bei der Datenverwendung bedienen, soweit deren Tätigkeit für den Schaden ursächlich war.

(5) Die gerichtliche Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 28 Abs. 3.

6. Abschnitt

KONTROLLORGANE

DATENSCHUTZKOMMISSION UND DATENSCHUTZRAT

§ 30. 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.

AUFGABEN DER DATENSCHUTZKOMMISSION

§ 31. (1) (Verfassungsbestimmung) Die Datenschutzkommission entscheidet:

1. **über Beschwerden von Personen, die behaupten, in ihrem Recht auf Auskunftserteilung (§ 23) verletzt zu sein;**
2. **über Beschwerden von Personen, die behaupten, in anderen Rechten nach diesem Bundesgesetz verletzt zu sein, soweit das verletzende Verhalten einem Rechtsträger des öffentlichen Rechts oder einem in Vollziehung der Gesetze tätigen Rechtsträger des privaten Rechts zuzurechnen ist und soweit dieses Verhalten nicht ein Akt der Gerichtsbarkeit oder der Gesetzgebung ist;**
3. **über die Verpflichtung eines Auftraggebers des öffentlichen Bereichs zur Anbringung oder Aufrechterhaltung eines Bestreitungsvermerks;**
4. **in Verfahren, die mit der Eintragung in das Datenverarbeitungsregister zusammenhängen;**
5. **über die Erteilung einer Genehmigung für den internationalen Datenverkehr;**

(2) Die Datenschutzkommission führt das Register der meldepflichtigen Datenverarbeitungen (§§ 14 bis 18) und prüft die Richtigkeit und Vollständigkeit von Registrierungen einschließlich des zugrundeliegenden Sachverhalts von amts wegen gemäß § 19.

(3) Die Datenschutzkommission übt die Kontrolle über Datenverarbeitungen gemäß § 26 aus und erstattet Empfehlungen an Auftraggeber von Datenverarbeitungen im Rahmen dieser Kontrolltätigkeit. Die Datenschutzkommission übt diese Kontrolltätigkeit über jede Datenverwendung im Inland unabhängig davon aus, ob die Frage der Rechtmäßigkeit der Datenverwendung nach österreichischem Recht zu beurteilen ist.

(4) Die Datenschutzkommission erstattet spätestens alle zwei Jahre einen Bericht über ihre Tätigkeit, der zu veröffentlichen ist.

(5) Die Datenschutzkommission ist zu allen Verordnungen anzuhören, die auf der Grundlage dieses Bundesgesetzes erlassen werden oder sonst Fragen des Datenschutzes berühren.

(6) Der Datenschutzkommission obliegen darüber hinaus die ihr sonst durch Gesetz übertragenen Aufgaben.

ZUSAMMENSETZUNG DER DATENSCHUTZKOMMISSION

§ 32. (1) Die Datenschutzkommission besteht aus vier Mitgliedern, die auf Vorschlag der Bundesregierung vom Bundespräsidenten für die Dauer von fünf Jahren bestellt werden. Wiederbestellungen sind zulässig. Ein Mitglied muß dem Richterstand angehören. Die Mitglieder sollen berufliche Erfahrung auf dem Gebiet des Datenschutzes aufweisen.

(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 Gerichtshofes für das richterliche Mitglied;
2. einen Vorschlag der Länder für zwei Mitglieder.

(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 eines Mitgliedes an dessen Stelle.

(5) Der Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;
2. Personen, die mit der Verarbeitung von Daten, auf die die Bestimmungen dieses Bundesgesetzes Anwendung finden, unmittelbar befaßt sind;
3. 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 zwei ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden.

(7) Auf die Ersatzmitglieder finden die Abs. 2, 3, 5 und 6 sinngemäß Anwendung.

(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 Absätze 2 und 3 ist für diese Zeit ein neues Mitglied zu bestellen.

(9) Die Mitglieder der Datenschutzkommission haben Anspruch auf Ersatz der Reisekosten (Gebührenstufe 5) nach Maßgabe der für Bundesbeamte der Allgemeinen Verwaltung 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 MITGLIEDER DER DATENSCHUTZKOMMISSION UND VERSCHWIEGENHEITSPFLICHT

§ 33. (Verfassungsbestimmung)

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

(2) Die Mitglieder der Datenschutzkommission unterliegen der Amtsverschwiegenheit und sind auch nach dem Ausscheiden aus ihrem Amt an die Verschwiegenheit gebunden.

ORGANISATION UND GESCHÄFTSFÜHRUNG DER DATENSCHUTZKOMMISSION

§ 34. (1) **(Verfassungsbestimmung)** Die Datenschutzkommission gibt sich eine Geschäftsordnung, 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. 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. Die in diesem Bereich tätigen Bediensteten unterstehen fachlich nur den Weisungen des Vorsitzenden oder des geschäftsführenden Mitglieds der Datenschutzkommission.

BESCHLÜSSE DER DATENSCHUTZKOMMISSION

§ 35. (**1) Die Datenschutzkommission faßt ihre Beschlüsse in Anwesenheit aller vier Mitglieder. Im Falle der Verhinderung eines Mitglieds nimmt das entsprechende Ersatzmitglied an der Beschlußfassung teil.**

(2) Das richterliche Mitglied führt den Vorsitz in der Datenschutzkommission.

(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 in geeigneter Weise zu veröffentlichen. Die näheren Vorkehrungen für die Veröffentlichung der Entscheidungen trifft die Datenschutzkommission.

WIRKUNG VON BESCHEIDEN DER DATENSCHUTZKOMMISSION

§ 36. (1) Gegen Bescheide, die das geschäftsführende Mitglied für die Datenschutzkommission gemäß § 17 Abs. 3 oder § 19 Abs. 3 iVm § 34 Abs. 1 erlassen hat, ist die Vorstellung an die Datenschutzkommission gemäß § 57 Abs. 2 AVG zulässig. Vorstellung kann auch das zuständige oberste Organ einer Gebietskörperschaft erheben, wenn sich der Bescheid gegen ein ihr unterstehendes Organ richtet. Eine Vorstellung gegen einen gemäß § 19 Abs. 3 ergangenen Bescheid hat aufschiebende Wirkung.

(2) Gegen die nicht dem Abs. 1 unterfallenden 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 zulässig.**

(3) Auftraggeber des öffentlichen Bereichs können Bescheide der Datenschutzkommission, welche im Registrierungsverfahren gemäß § 15 Abs. 5 oder gemäß § 17 Abs. 2 ergangen sind oder mit welchen gemäß § 11 eine beantragte Genehmigung verweigert wurde, durch Amtsbeschwerde des zuständigen obersten Organs vor dem Verwaltungsgerichtshof bekämpfen. Die Beschwerde besitzt im Falle des § 15 Abs. 5 aufschiebende Wirkung, im Falle des § 17 Abs. 2 nur dann, wenn die Ablehnung der Registrierung keine Datenverarbeitung gemäß § 15 Abs. 2 betrifft.

(4) Wenn die Datenschutzkommission eine Verletzung von Bestimmungen dieses Bundesgesetzes durch einen Auftraggeber des öffentlichen Bereichs festgestellt hat, so ist der Auftraggeber der geprüften Datenverarbeitung, **sofern kein Rechtsmittel mit aufschiebender Wirkung ergriffen wurde**,verpflichtet, mit den ihm zu Gebote stehenden rechtlichen Mitteln unverzüglich den der Rechtsanschauung der Datenschutzkommission entsprechenden Zustand herzustellen.

EINRICHTUNG UND AUFGABEN DES DATENSCHUTZRATES

§ 37. (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. **haben Auftraggeber des öffentlichen Bereichs ihre Vorhaben, soweit sie wesentliche Auswirkungen auf den Datenschutz in Österreich haben, dem Datenschutzrat zur Stellungnahme zuzuleiten;**
3. **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;**
4. **kann der Datenschutzrat Auftraggeber des privaten Bereichs oder auch ihre gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung auffordern, die aus datenschutzrechtliche Sicht Anlaß zu Bedenken, zumindest aber Anlaß zur Beobachtung geben;**
5. **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.**

ZUSAMMENSETZUNG DES DATENSCHUTZRATES

§ 38. (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) § 32 Abs. 5 über die Unvereinbarkeit ist sinngemäß anzuwenden.

(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis sie auf eigenen Wunsch ausscheiden oder von den entsendenden Stellen (Abs. 1) andere Vertreter namhaft gemacht worden sind.

(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 5) nach Maßgabe der für Bundesbeamte der Allgemeinen Verwaltung geltenden Rechtsvorschriften.

VORSITZ UND GESCHÄFTSFÜHRUNG DES DATENSCHUTZRATES

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

(2) Der Datenschutzrat wählt aus seiner Mitte einen Vorsitzenden und zwei stellvertretende Vorsitzende. Die Funktionsperiode des Vorsitzenden (stellvertretenden Vorsitzenden) dauert fünf Jahre, wenn jedoch der Vorsitzende **gemäß § 38 Abs. 5 bereits früher aus dem Datenschutzrat ausscheidet, nur bis zu diesem Zeitpunkt. Wiederbestellungen sind zulässig.**

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

SITZUNGEN UND BESCHLUßFASSUNG DES DATENSCHUTZRATES

§ 40. (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.

(4) Die Beifügung von Minderheitenvoten ist zulässig.

(5) 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.

(6) Jedes Mitglied des Datenschutzrates ist verpflichtet, an den Sitzungen - außer im Fall der gerechtfertigten Verhinderung - teilzunehmen. Jedes Mitglied hat seine Verhinderung an der Teilnahme rechtzeitig bekanntzugeben, worauf das Ersatzmitglied einzuladen ist.

(7) 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.

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

7. Abschnitt

BESONDERE VORSCHRIFTEN FÜR EINZELNE KATEGORIEN VON DATENVERARBEITUNGEN

SENSIBLE DATEN (Verfassungsbestimmung)

§ 41. (1) Sensible Daten dürfen jedenfalls verwendet werden, wenn dies

1. **erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeitsrechts Rechnung zu tragen; die näheren Bestimmungen sind in den arbeitsrechtlichen Vorschriften enthalten;**
2. **zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verarbeitung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen;**
3. **zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor den zuständigen Behörden erforderlich ist und wenn der Auftraggeber die Daten rechtmäßig ermittelt hat;**
4. **zur Wahrung lebenswichtiger Interessen eines anderen Menschen unerläßlich ist.**

(2) Nicht auf Gewinn gerichtete Vereinigungen mit politischem oder weltanschaulichem Tätigkeitszweck dürfen Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten, soweit es sich um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben. Diese Daten dürfen nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

DATEN ÜBER VERURTEILUNGEN

§ 42. Datenverarbeitungen mit Daten über Straftaten, strafrechtliche Verurteilungen oder vorbeugende Maßnahmen dürfen nur vorgenommen werden, wenn dies durch Gesetz ausdrücklich vorgesehen ist.

ZURVERFÜGUNGSTELLUNG VON ADRESSEN

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

(2) Soll die Übermittlung

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

2. aus einem öffentlichen Benachrichtigungsinteresse oder
3. zum Zweck der Befragung der Betroffenenen für wissenschaftliche oder statistische Zwecke

erfolgen und würde die Einholung der Zustimmung der Betroffenen einen unverhältnismäßigen Aufwand erfordern, ist eine Übermittlung mit Genehmigung der Datenschutzkommission zulässig, wenn der Antragsteller das Vorliegen einer der in Z 1 bis 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Ist das Auswahlkriterium für den Betroffenenkreis ein sensibles Datum, muß das Vorliegen eines wichtigen öffentlichen Interesses nachgewiesen werden. Die Datenschutzkommission hat zur Wahrung der schutzwürdigen Interessen der Betroffenen die Genehmigung mit den notwendigen Bedingungen und Auflagen zu verbinden; dies gilt insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium.

(3) Die übermittelten Adreßdaten dürfen ausschließlich für den im Genehmigungsantrag genannten Zweck verwendet werden und sind zu löschen, sobald sie für die Benachrichtigung oder Untersuchung nicht mehr benötigt werden.

(4) In jenen Fällen, in welchen es gemäß den vorstehenden Bestimmungen zulässig ist, Namen und Adresse von Personen, die einem bestimmten Betroffenenkreis angehören, zu übermitteln, darf die Ermittlung und Verarbeitung dieser Adreßdaten zum Zweck der Auswahl der zu übermittelnden Daten erfolgen.

PUBLIZISTISCHE TÄTIGKEIT

§ 44. (1) Soweit Medienunternehmen, Mediendienste oder Medienmitarbeiter Daten unmittelbar für ihre publizistische Tätigkeit im Sinne des Mediengesetzes, BGBl. Nr. 314/1981, verwenden, finden von den einfachgesetzlichen Bestimmungen dieses Bundesgesetzes nur die §§ 2 bis 4, 8, 9, 12 und 13 Anwendung sowie § 5 mit der Maßgabe, daß die in § 5 Abs 2 enthaltenen Verwendungsbeschränkungen für veröffentlichte Daten nicht gelten.

(2) Die Ermittlung, Verarbeitung und Übermittlung von Daten für Tätigkeiten nach Abs. 1 ist insoweit zulässig, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und Medienmitarbeiter in Ausübung des Grundrechtes auf freie Meinungsäußerung gemäß Art. 10 Abs. 1 EMRK, BGBl. Nr. 210/1958, erforderlich ist.

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

AUTOMATISIERTE EINZELENTSCHEIDUNGEN

§ 45. (1) Die Beurteilung von Eigenschaften, Fähigkeiten oder Lebensverhältnissen von natürlichen Personen allein aufgrund eines automationsunterstützt ablaufenden Bewertungsverfahrens ist, soferne sich daraus nachteilige Folgen für den Betroffenen ergeben können, ohne nachprüfende Kontrolle durch einen Sachbearbeiter und die Einräumung der Möglichkeit zur Stellungnahme durch den Betroffenen nicht zulässig.

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

INFORMATIONSVERBUNDSYSTEME

§ 46. (1) Die gemeinsame Verarbeitung von Daten mehrerer Auftraggeber mit demselben Tätigkeitsbereich in der Art, daß alle teilnehmenden Auftraggeber auf die Gesamtheit der verarbeiteten Daten Zugriff haben, ist dann, wenn sie aufgrund ihres Zwecks geeignet ist, für die Betroffenen nachteilige Folgen zu bewirken, nur aufgrund ausdrücklicher gesetzlicher Ermächtigung im Sinne des § 6 Abs. 1 zulässig.

(2) Bei jedem Informationsverbundsystem haben die Auftraggeber einen Betreiber des Systems zu bestimmen und in der Meldung an die Datenschutzkommission zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Dieser Betreiber vertritt gegenüber den Betroffenen die Auftraggeber und hat, falls ein Betroffener sich nicht direkt an einen Auftraggeber wendet, den Betroffenen gegenüber alle Auftraggeberpflichten wahrzunehmen. Den Betreiber trifft die Verantwortung für die Organisation und Durchführung der Eingabe, Ausgabe und Veränderung von Daten des Systems.

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

8. Abschnitt

STRAFBESTIMMUNGEN

DATENBESCHAFFUNG IN SCHÄDIGUNGSABSICHT

§ 47. (1) Wer einem anderen in seinen Rechten dadurch absichtlich einen Schaden zufügt, daß er Daten verwendet, die er sich aus einer Datenverarbeitung **unbefugt** verschafft 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 oder auf Antrag der Datenschutzkommission zu verfolgen.

VERWALTUNGSSTRAFBESTIMMUNG

§ 48. (1) Eine Verwaltungsübertretung, die mit Geldstrafe bis zu 150 000 S zu ahnden ist, begeht, wer

1. **rechtswidrige Anordnungen im Sinne des § 13 Abs. 3 zur Übermittlung von Daten erteilt, wobei ihm zumindest grobe Fahrlässigkeit vorzuwerfen ist;**
2. **Daten in Verletzung des Datengeheimnisses (§ 13 Abs. 1) übermittelt;**
3. **Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht;**
4. **Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 15 erfüllt zu haben;**
5. **Daten ins Ausland übermittelt oder überläßt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 11 eingeholt zu haben,**
6. **die gemäß § 12 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht läßt,**
7. **seine Informationspflichten gemäß den §§ 20, 21 oder 22 verletzt,**
8. **seiner Verpflichtung zur Beantwortung eines Auskunftsbegehrens gemäß § 23 Abs. 5 nicht entspricht,**
9. **Daten entgegen § 23 Abs. 6 löscht.**

(2) Wird die Tat von einem Auftraggeber des öffentlichen Bereichs begangen, ist jener Organwalter verantwortlich, der nach den internen Organisationsvorschriften (Geschäftseinteilung und Geschäftsordnung) zur Entscheidung über die rechtswidrige Datenverwendung oder für die Vornahme der unterlassenen Handlung zuständig war.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern und Programmen kann ausgesprochen werden (§§ 10, 17 und 18 VStG 1950), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 in Zusammenhang stehen.

(5) Zuständig für Entscheidungen nach Abs. 1 bis 4 ist die **Bezirksverwaltungsbehörde**.

9. Abschnitt

ÜBERGANGS- UND SCHLUSSBESTIMMUNGEN

BEFREIUNG VON
GEBÜHREN, ABGABEN UND VOM KOSTENERSATZ

§ 49. (1) Die durch dieses Bundesgesetz unmittelbar veranlaßten Eingaben der Betroffenen zur Wahrung ihrer Interessen sowie die Eingaben im Registrierungsverfahren und die gemäß § 18 Abs. 2 zu erstellenden Registerauszüge sind von den Stempelgebühren und von den Verwaltungsabgaben des Bundes befreit.

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

MITTEILUNGEN AN DIE ANDEREN MITGLIEDSTAATEN DER EUROPÄISCHEN UNION UND AN DIE EUROPÄISCHE KOMMISSION

§ 50. (1) Von der Erlassung eines Gesetzes, 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 § 11 Abs. 2 Z 1 nicht als gegeben erachtet wurden;**
2. **der Datenverkehr in ein Drittland ohne angemessenes Datenschutzniveau genehmigt wurde, weil die Voraussetzungen des § 11 Abs. 2 Z 2 als gegeben erachtet wurden.**

FESTSTELLUNGEN DER EUROPÄISCHEN KOMMISSION

§ 51. Der Inhalt der in einem Verfahren gemäß Art. 31 Abs. 2 der Richtlinie 95/46/EG getroffenen Feststellungen der Europäischen Kommission über

1. **das Vorliegen oder Nichtvorliegen eines angemessenen Datenschutzniveaus in einem Drittland oder**
2. **die Eignung bestimmter Standardvertragsklauseln zur Gewährleistung eines angemessenen Schutzes der Datenverwendung in einem Drittland**

ist vom Bundeskanzler im Bundesgesetzblatt gemäß § 2 Abs. 3 BGBlG, BGBl. Nr. 660/1996, mit verbindlicher Wirkung kundzumachen.

INKRAFTTRETEN

§ 52. (1) (Verfassungsbestimmung) Die Verfassungsbestimmungen des § 1, § 2, § 31 Abs. 1, § 33, § 34 Abs. 1 und des § 41 treten mit 24. Oktober 1998 / Variante: 1. Jänner 1999 / in Kraft.

(2) Die übrigen Bestimmungen dieses Bundesgesetzes treten ebenfalls mit 24. Oktober 1998 / Varainte: 1. Jänner 1999 / in Kraft.

(3) (Verfassungsbestimmung) Mit dem Inkrafttreten dieses Bundesgesetzes tritt das Datenschutzgesetz, BGBl. Nr. 565/1978, außer Kraft.

ÜBERGANGSBESTIMMUNGEN

§ 53. (1) Vor Inkrafttreten dieses Bundesgesetzes durchgeführte Registrierungen im Datenverarbeitungsregister gelten als Registrierungen im Sinne des § 18 weiter, es sei denn, daß es sich um Datenverarbeitungen mit dem in § 15 Abs. 2 genannten Inhalt handelt. Für solche Datenverarbeitungen ist bis spätestens 1. Jänner 2001 eine neue Meldung gemäß § 15 Abs. 2 zu erstatten. Die Weiterführung der Verarbeitung ist bis zur rechtskräftigen Entscheidung über die Registrierung zulässig.

(2) Vor Inkrafttreten dieses Bundesgesetzes erteilte Genehmigungen im internationalen Datenverkehr müssen vor dem 1. Jänner 2001 neu beantragt werden, soweit eine Genehmigung gemäß § 11 erforderlich ist. Bis zur rechtskräftigen Entscheidung über den

Genehmigungsantrag dürfen die vor Inkrafttreten dieses Bundesgesetzes genehmigten Übermittlungen und Überlassungen ins Ausland fortgeführt werden.

(3) In Verfahren über behauptete Datenschutzverletzungen, die vor dem Inkrafttreten dieses Bundesgesetzes eingeleitet wurden, ist, sofern es sich um die Feststellung der Rechtmäßigkeit oder Rechtswidrigkeit eines Sachverhalts oder das Vorliegen eines strafbaren Tatbestands handelt, die Rechtslage zum Zeitpunkt der Verwirklichung des Sachverhalts maßgebend; soweit es sich um das Bestehen einer Verpflichtung zu einer Leistung oder Unterlassung handelt, ist die Rechtslage im Zeitpunkt der Entscheidung in erster Instanz zugrundezulegen.

VOLLZIEHUNG

§ 54. 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

1. 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. 0031-0050; CELEX-Dokumentnummer: 395L0046) ist diese Richtlinie bis spätestens 24. Oktober 1998 in der österreichischen Rechtsordnung umzusetzen.

2 Lösung

Neues Datenschutzgesetz zum Zweck

1. der Umsetzung der Richtlinie und
2. der Einarbeitung jenes Änderungsbedarfes, der sich aus den Anwendungserfahrungen hinsichtlich des DSG , BGBl. Nr. 565/1978 idgF, ergeben hat

3. Alternativen

keine

4. Kosten: verursacht durch

1. zusätzliche Kompetenzen der Datenschutzkommission:
   4 Planstellen (1 Informatiker (A/a), 2 Juristen, 1 Sekretariatskraft)
2. elektronische Registrierung:
   jedenfalls 8 - 10 Mio. S; Projektumfang ist jedoch noch nicht abgeklärt
3. Entfall der Registrierungsgebühr:
   etwa S 500.000,-- unter Berücksichtigung des Umstandes, daß Standardverarbeitungen nicht mehr registrierungspflichtig sein sollen.

5. EU-Konformität

gegeben, da Richtlinienumsetzung

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. Dementsprechend hat Österreich bis 24. Oktober 1998 die **notwendigen Anpassungen im Datenschutzrecht** vorzunehmen.

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-Daten-schutzrichtlinie-Kommentar, 1997, S. 65).

2. Es wurde ursprünglich davon ausgegangen, daß eine **Novelle zum Datenschutzgesetz**, BGBl. Nr. 565/1978, zur Umsetzung genügen werde. In den Vorberatungen 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) aufrecht erhalten wurde.

3. Auch wenn es sich um ein neues Gesetz handelt, wurde dennoch versucht, **bewährte Regelungsstrukturen grundsätzlich aufrecht zu erhalten**. Es gibt daher nach wie vor ein Grundrecht auf Datenschutz (§ 1), das in umfangreichen einfachgesetzlichen Bestimmungen (§§ 3-54) ausgeführt wird. Als Neuerung im Grundrecht ist der ausdrückliche, besondere Schutz für sensible Daten zu erwähnen (§ 1 Abs. 3): 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 (z.B. in Karteien, Listen etc.) 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 Art. 6, 7 und 8 der Richtlinie entsprechend zu berücksichtigen waren. Wie in der Richtlinie vorgezeichnet, wird nunmehr den Bestimmungen über die Zulässigkeit der Datenverwendung ein Katalog von „**Grundsätzen für die Datenqualität**“ vorangestellt, der die obersten Prinzipien rechtmäßigen Umgangs mit personenbezogenen Daten enthält.

5. Die Forderung nach möglichster **Publizität von Datenverarbeitungen** wurde in dem von der Richtlinie erforderlichen Ausmaß erweitert. 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 die Datenverarbeitung seiner Vertragspartner einfließen.

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

7. Wesentliche **Änderungen** mußten in Umsetzung der Richtlinie 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 bestimmten Arten von Datenverarbeitungen der Datenverkehr mit dem Ausland ohne Beschränkungen zulässig. Für alle anderen Kategorien von Datenverarbeitungen ist jeweils die Angemessenheit des Datenschutzniveaus im Empfängerstaat (beim Empfänger) zu prüfen. 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 haben 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, d.h. 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 Fällen, in welchen nicht einmal die schutzwürdigen Geheimhaltungsinteressen natürlicher Personen gefährdet erscheinen, davon auszugehen sein wird, daß auch die schutzwürdigen Geheimhaltungsinteressen juristischer Personen nicht ernstlich gefährdet sind.

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

- Die neue Informationspflicht des Auftraggebers macht dem Betroffenen bewußt, daß seine Geheimhaltungsinteressen berührt sind;
- das Auskunftsrecht, das als Angelpunkt für die Verwirklichung von Betroffeneninteressen anzusehen ist, ist in Hinkunft leichter durchsetzbar, da hiefür nunmehr immer die Datenschutzkommission zuständig ist;
- die unabhängige Kontrollstelle (in Österreich: die Datenschutzkommission) kann alle Datenverarbeitungen überprüfen;
- 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 Durchsetzung der Interessen 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, zu Entscheidungen über Verletzungen des Datenschutzes im privaten Bereich sind die ordentlichen Gerichte berufen.

Als **unabhängige Kontrollstelle iSd Art. 28** der Richtlinie wird die Datenschutzkommission eingesetzt, der die Kontrolle über sämtliche Auftraggeber einer Datenverarbeitung - soweit sie nicht der Gerichtsbarkeit oder der Gesetzgebung zuzurechnen ist - 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, die von der Ausübung der Entscheidungskompetenz wesentlich verschieden sind, wird eine gewisse Umstrukturierung des Geschäftsapparates der Datenschutzkommission zur Folge haben müssen. Die Zurverfügungstellung der notwendigen Ressourcen ist gemäß § 34 Abs. 2 Aufgabe des Bundeskanzlers.

10. Wesentliche Neuerungen bringt der Entwurf schließlich im Bereich der **Strafbestimmungen**. Dieser Bereich ist aus heutiger Sicht 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) jedem 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. An Stelle des gerichtlich strafbaren Tatbestands wurde daher ein Verwaltungsstraftatbestand geschaffen, der eine ausreichende Sanktion enthält, ohne zur ungerechtfertigten Kriminalisierung der arbeitenden Bevölkerung beizutragen. Beibehalten als gerichtlich strafbare Handlung wurde jedoch das Absichtsdelikt der Schädigung mit Hilfe von unrechtmäßig beschafften Daten (§ 47).

Im Gegenzug zur Modernisierung der gerichtlich strafbaren Tatbestände wurden die Verwaltungsstrafbestimmungen ausgedehnt auf jene Fälle, in welchen eine Durchsetzung des Rechtes auf gesetzmäßiges Verhalten nicht im Wege einer Beschwerde oder Klage erfolgen kann, weil kein subjektives Recht des Betroffenen vorliegt, sodaß eine Sanktion durch Bestrafung bei Zuwiderhandeln notwendig erscheint.

11. Für die **Umstellung bestehender Datenverarbeitungen** auf die neue Rechtslage, setzt die Richtlinie eine weitere **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 Datenverarbeitungen und angesichts des Umstandes, daß nur ein geringer Prozentsatz des internationalen Datenverkehrs nicht unter Art. 26 Abs. 1 RL fällt und daher nicht genehmigungsfrei ist.

12. Zur **Kompetenzgrundlage** des Entwurfs ist folgendes auszuführen:
Im vorliegenden Text wird deshalb keine Aussage über die verfassungsrechtliche Kompetenz zur Gesetzgebung und Vollziehung in Angelegenheiten des Datenschutzes getroffen, weil es wünschenswert wäre, die diesbezüglichen Bestimmungen den Art. 10 - 15 B-VG einzugliedern.
Was den Inhalt dieser Bestimmungen betrifft, sollte in Gesprächen mit den Ländern versucht werden, die derzeit geltende Kompetenzgrundlage für das DSG so zu gestalten, daß eine vollständige Umsetzung der Richtlinie durch Bundesgesetz möglich ist.

13. Für die finanziellen Auswirkungen des vorliegenden Gesetzentwurfes sind die folgenden Komponenten maßgebend:
a) Ins Gewicht fallende **Folgekosten** würden sich bei einer Gesetzwerdung dieses Entwurfs zunächst 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 4 zusätzliche Planstellen zur Verfügung gestellt werden müßten (1 weiterer Informatiker (A/a) und 2 Juristen, sowie eine Sekretariatskraft), wenn kein allzu krasses Vollzugsdefizit entstehen soll. Dies würden Kosten von etwa 4 Mio. S pro Jahr bedeuten.
Ob die neue Zuständigkeit der Datenschutzkommission für Beschwerden über die Verletzung der Auskunftspflicht im privaten Bereich besonderen zusätzlichen Arbeitsanfall bedeutet, bleibt abzuwarten. Schon bisher konnten in der „Schlichtungsstelle-Datenschutz“ im Bundeskanzleramt derartige Beschwerden anhängig gemacht werden. In den letzten Jahren wurden jeweils weniger als 50 Fälle an das Bundeskanzleramt herangetragen.

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. Genauere Aussagen über die Umstellungskosten können derzeit noch nicht gemacht werden, doch werden voraussichtlich 8 - 10 Mio. S für die Programmentwicklungs- und Implementierungskosten anzusetzen sein.

Als elektronische Infrastruktur für die „Registrierung via Netz“ könnte das im Ausbau begriffene „Help“-Projekt der Bundesverwaltung dienen, das Zugang zur öffentlichen Verwaltung über elektronsiche Netze verschafft.

Mit signifikanten zusätzlichen Vollzugskosten durch die **Ausweitung der Registrierungspflicht auf manuelle Dateien** ist deshalb nicht zu rechnen, weil die Zahl solcher registrierungspflichtiger Dateien heute bereits gering sein dürfte und in Zukunft noch weiter abnehmen wird. Wenn weiters bedacht wird, daß im privaten Bereich viele dieser Karteien von Standardverarbeitungen umfaßt sind, wird deutlich, daß der zusätzliche Registrierungsbedarf nicht bedeutend sein wird. Falls sich ergeben sollte, daß in bestimmten Bereichen Handkarteien in beträchtlichem Ausmaß in Gebrauch sind, wird auch die Möglichkeit der Schaffung neuer Standardverarbeitungen zu prüfen sein.
Freilich wird die Höhe dieser Vollzugskosten auch davon abhängen, wie die Frage der Gesetzgebungs- und Vollziehungskompetenz gelöst wird.

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

Zusätzlicher **Registrierungsbedarf** wird gemäß der Übergangsbestimmungen bei jenen Datenverarbeitungen entstehen, die der Vorabkontrolle unterliegen; dies sind voraussichtlich etwa 5% - 10% der vorhandenen Registrierungen.
Dieser zusätzlich Aufwand sollte in etwa wettgemacht werden durch den künftigen Entfall der Registrierungspflicht für Standardverarbeitungen; dies sind derzeit 30 % der vorhandenen Registrierungen.

Die Einholung neuer **Genehmigungen** im Datenverkehr mit Drittstaaten wird ebenfalls keinen besonderen Aufwand bedeuten, weil die meisten Datenexportkategorien des täglichen Geschäftslebens ohnehin durch § 10 Abs. 3 von der Genehmigungspflicht ausgenommen sind und der Datenverkehr mit EU-Staaten durch § 10 Abs. 1 und 2 liberalisiert ist (was sich mit Hilfe der Verordnungsermächtigung im § 10 Abs. 2 voraussichtlich auch für die Daten juristischer Personen erzielen lassen wird).

Kosten werden weiters für die neue **Informationspflicht** der Auftraggeber anfallen. Wenn aber bedacht wird, daß pro Jahr im Durchschnitt 5000 - 7000 neue Registrierungen erfolgen, wovon 30 % auf Standardverarbeitungen entfallen - für die nach dem vorliegenden Entwurf keine Informationspflicht entsteht - wird deutlich, daß die Informationspflicht für neue Datenverarbeitungen keinen wesentlichen Kostenfaktor darstellen wird.

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 von über ihn ermittelten Daten an Dritte zu verstehen.

Freilich kann dieser Anspruch nicht ohne Einschränkungen bestehen:
Schon **Absatz 1** erkennt das Recht auf Datenschutz nur dann zu, wenn der Betroffene selbst ein schutzwürdiges Geheimhaltungsinteresse hat. Ein solches ist jedenfalls in folgenden Fällen nicht gegeben:
2.1.1 Ein Geheimhaltungsinteresse des Betroffenen selbst kann dann nicht vorliegen, wenn er ein gegenüber dem Geheimhaltungsinteresse überwiegendes Interesse an der Verwendung seiner Daten hat. Dies ist z.B. zweifellos dann der Fall, wenn ein lebenswichtiges - z.B. gesundheitliches - Interesse des Betroffenen die Benützung seiner Daten - z.B. für seine ärztliche Behandlung - erfordert.
Ein Geheimhaltungsinteresse des Betroffenen besteht aber auch dann nicht, wenn er durch Erteilung seiner Zustimmung zu einer bestimmten Verwendung seiner Daten dargetan hat, daß er ein solches Interesse in einem bestimmten Zusammenhang für nicht gegeben erachtet.
Ein schutzwürdiges Geheimhaltungsinteresse kann nicht an Daten bestehen, die allgemein zugänglich sind aufgrund einer - rechtlich zulässigen - Veröffentlichung: Was bekannt ist oder zumindest jederzeit in Erfahrung gebracht werden kann, kann nicht „geheim gehalten“ werden. Um dem im Grundrechtsbereich immer anzuwendenden Verhältnismäßigkeitsgebot voll zu genügen, bedarf der Grundsatz, daß an veröffentlichten Daten kein schutzwürdiges Geheimhaltungsinteresse besteht, freilich noch gewisser verfeinernder Korrekturen, die im § 5 Abs. 2 des vorliegenden Entwurfs vorgenommen werden (vgl. die Erläuterungen a.a.O.).

Auch in Fällen, in welchen nach den vorstehenden Ausführungen davon auszugehen ist, daß ein schutzwürdiges Geheimhaltungsinteresse gegeben ist, kann dieses dennoch nicht immer verwirklicht werden und zwar dann nicht, wenn überwiegende berechtigte Interessen des Staates oder eines Dritten vorliegen: Die Absätze 2 und 3 des § 1 definieren die im Interesse des Staates oder im Interesse Dritter zulässigen Eingriffstatbestände, wobei in **Absatz 2** die bisher geltende Regelung aufrechterhalten wird.

Nur hinsichtlich der sogenannten „sensiblen Daten“ (vgl. hiezu die Definition in § 1 Abs. 3 sowie in § 3 Z 2) ergibt sich dabei eine Neuerung gegenüber der bisherigen Rechtslage: **Absatz 3** setzt das grundsätzliche Verarbeitungsverbot der Richtlinie 95/46/EG für sensible

Daten (Art. 8 Abs. 1) um. Ausnahmen hievon dürfen - richtlinienkonform - generell nur dann stattfinden, wenn sie auf Gesetzen beruhen, die aufgrund wichtiger öffentlicher Interessen notwendig sind (Art. 8 Abs. 4 der Richtlinie). Die übrigen Ausnahmetatbestände vom Verarbeitungsverbot für sensible Daten, die in Art. 8 der Richtlinie enthalten sind, sind im vorliegenden Entwurf einerseits in § 40 umgesetzt, soweit es sich um Ausnahmen im Interesse der Rechten und Freiheiten Dritter handelt, andrerseits in den §§ 6 und 7 (näherhin § 6 Abs. 4 Z 1 und 2 und § 7 Abs. 1 Z 2 und 3), soweit die Interessenslage des Betroffenen selbst einem Verwendungsverbot entgegensteht.
Aus der Sicht der österreichischen Verfassungsrechtslage ist folgendes hinzuzufügen: Während § 40 im Range einer Verfassungsbestimmung stehen muß, weil er Ausnahmetatbestände (im Interesse Dritter) enthält, die nicht unter die nach § 1 Abs. 3 DSG 1998 zulässigen Ausnahmetatbestände (aus wichtigen öffentlichen Interessen) subsumiert werden können, ist eine Beschlußfassung im Verfassungsrang über die Bestimmungen des § 6 Abs. 4 Z 1 und 2 und des § 7 Abs. 1 Z 2 und 3 nicht erforderlich, weil diese, in der Interessenslage des Betroffenen selbst begründeten Ausnahmen vom Grundrecht auf Datenschutz gar nicht erfaßt sind (vgl. die Ausführungen zu Abs. 1).

§ 1 Abs. 4 enthält die richtliniengemäße Ausdehnung des Rechtes auf Auskunft und Richtigstellung bzw. Löschung auf manuelle Dateien und berücksichtigt das Widerspruchsrecht (§ 25) als möglichen Grund für einen Löschungsanspruch.

Im **Absatz 6 des § 1** wird die für das österreichische Datenschutzrecht traditionelle Teilung des Rechtsschutzinstrumentariums zwischen ordentlichen Gerichten und Datenschutzkommission in einer Weise vorgenommen, 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.

Zu § 2 des Entwurfs (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 österreichisches Recht anzuwenden ist.
Ausnahmen bestehen zugunsten des im Gemeinschaftsrecht angesichts der Dienstleistungsfreiheit bestehenden Sitzstaatsprinzips dann, wenn eine Datenverarbeitung in Österreich aus einem anderen EU-Staat her betrieben wird, ohne daß der Auftraggeber (der seinen Sitz in einem anderen EU-Staat hat) in Österreich eine feste Betriebsstätte („Niederlassung“ iSd § 3 Z 16) hätte. Umgekehrt gilt österreichisches Datenschutzrecht in einem anderen EU-Staat dann, wenn von einer „Niederlassung“ (iSd § 3 Z 16) in Österreich aus, Datenverarbeitung im EU-Ausland betrieben wird.

Der Ort der Niederlassung des Auftraggebers ist somit der maßgebliche Anknüpfungspunkt der Anwendbarkeit der innerstaatlichen Rechtsordnung, soweit es sich um Datenverarbeitungen für einen Auftraggeber mit Sitz in einem EU-Mitgliedstaat handelt. Bei Datenverarbeitungen für Zwecke eines Auftraggebers, der keinen Sitz in einem EU-Mitgliedsstaat hat, gilt hingegen immer der Ort der Datenverwendung als Anknüpfungspunkt für die Anwendbarkeit einer nationalen Rechtsordnung.

Zu § 3 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 DSG notwendig war.

Angesichts der Definition des Begriffs „Daten“ in der Richtlinie mußte im vorliegenden Entwurf (**Z 1**) die 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 (z.B. den Inhaber des Entschlüsselungscodes bei codierten Identitätsdaten) bestimmbar sind. Um hier eine sinnvolle Grenze zu ziehen, wird das Kriterium des „unverhältnismäßigen Aufwandes“ aus dem Erwägungsgrund 26 zur Richtlinie entnommen, wo es heißt, daß bei der Entscheidung, ob eine Person bestimmbar ist, alle Mittel berücksichtigt werden sollten, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.
Die Bestimmbarkeit „mit hoher Wahrscheinlichkeit“ hat sich in der Praxis als wenig bedeutsam erwiesen, weshalb diese Spezifikation in die Definition nicht mehr aufgenommen wurde.
Neu ist die taxative Aufzählung der „sensiblen Daten“ in **Z 2,** die in Umsetzung des Art. 8 Abs. 1 RL erfolgt.
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 § 6 Abs. 4 Z 4 (vgl. die Erläuterungen a.a.O.)
Die Ausdehnung der Definitionen von Auftraggeber und Dienstleister (**Z 4 und 5)** auch auf Personengemeinschaften entspricht einem Bedürfnis der Praxis. Doch mußte die Grenze der Ausweitung dieser Definition - schon im Hinblick auf allfällige Schadenersatzansprüche - bei der Möglichkeit der eindeutigen Zurechenbarkeit von Rechten und Pflichten (privater Bereich) bzw. gesetzlichen Zuständigkeiten (öffentlicher Bereich) gezogen werden.
Der Begriff der „Datenverarbeitung“ in der **Z 7** war im Hinblick auf die Definition der (automationsunterstützten) „Verarbeitung“ in Art. 2 lit. b der RL durch Weglassen des letzten Halbsatzes zu ändern: Für den Fall, daß eine Bundeskompetenz zur Regelung des Daten-

schutzes bei manuellen Dateien geschaffen werden sollte, ist eine entsprechende Ausweitung des Begriffs der „Datenverarbeitung“ in eckigen Klammern vorgesehen.
Wesentlich für das Begriffsinstrumentarium des Entwurfes ist jedenfalls die Unterscheidung des Begriffs der „Datenverarbeitung“ von dem Begriff des „Verarbeitens von Daten“. Die „Datenverarbeitung“ (**Z 7**) ist eine logische Einheit, die unterschiedlichste Handlungen umfaßt, wie etwa ermitteln (**Z 8**), verarbeiten (**Z 9**), übermitteln (**Z 12**), usw. Das verbindende Element ist der Gesamtzweck der Datenverarbeitung, zu dessen Erreichung die einzelnen Schritte gesetzt werden (**Z 9**).
„Verarbeiten“ hingegen ist nur eine bestimmte Kategorie von Handlungen, die - neben anderen Kategorien von Handlungen, die z.B. als „ermitteln“ zu qualifizieren sind - im Rahmen einer konkreten Datenverarbeitung gesetzt werden.
Der allumfassendste Begriff für das Umgehen mit Daten ist der Begriff „Verwenden“, der in der Z 14 definiert wird. Der Begriff des „Verwendens“ von Daten entspricht dem Begriff „Verarbeiten“ in der Richtlinie, in der definitorisch zwischen ermitteln, 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 „ermitteln“, „verarbeiten“ und „übermitteln“ unterschieden werden und dem Überbegriff „verwenden“ untergeordnet werden.

Zu § 4 des Entwurfs (öffentlicher und privater Bereich):

In Übereinstimmung mit § 1 Abs. 6 stellt die Abgrenzung zwischen Auftraggebern (Datenverarbeitungen) 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 § 5 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 - in sprachlich gekürzter Form - nunmehr auch in das DSG 1998 **(§ 5 Abs. 1)** aufgenommen . Da es vorkommen kann, daß diese Prinzipien nicht in jeder Phase einer Datenverarbeitung restlos erfüllt werden können (insbesondere die Forderung nach Richtigkeit der Daten), wird dieser Katalog von Grundsätzen im vorliegenden Entwurf als Sollensbestimmung formuliert. Jeder Auftraggeber hat die Pflicht, diese Ziele bei jeder seiner Datenverarbeitungen zu verwirklichen, wobei Abweichungen von der Zielerreichung nur durch sachliche Besonderheiten einzelner Datenverarbeitungen oder einzelner Phasen innerhalb einer Datenverarbeitung gerechtfertigt sein können.

Absatz 2 bringt die einfachgesetzliche Ausgestaltung des § 1 Abs. 1, und zwar insofern, als die Konsequenzen der mangelnden Schutzwürdigkeit von personenbezogenen Daten infolge ihrer öffentlichen Verfügbarkeit näher geregelt werden. Da dies eine Regelung von zentraler Bedeutung ist, wird sie in unmittelbarem Anschluß an die Grundsätze des Abs. 1 getroffen. Auch wenn die Richtlinie selbst keine ausdrücklichen Aussagen darüber enthält, wie mit veröffentlichten Daten datenschutzrechtlich umzugehen ist, kann aus der Sonderbestimmung über die Zulässigkeit der Verwendung veröffentlichter sensibler Daten (Art. 8 Abs. 2 lit. e) geschlossen werden, daß die Richtlinie generell davon ausgeht, daß die Verwendung von veröffentlichten Daten zulässig ist.
Daß eine solche Verwendungserlaubnis durch die Rechtmäßigkeit der Veröffentlichung begrenzt sein muß, liegt auf der Hand und ist auch insofern keine unrealistische Forderung, als die einmalige Veröffentlichung eines Datums noch lange nicht bedeutet, daß das Datum jedermann bekannt ist: Sobald die Rechtswidrigkeit einer Veröffentlichung festgestellt ist und in der Folge die Verfügbarkeit des Datum für die Öffentlichkeit beendet wird, ist eine „Geheimhaltung“, zumindest für die fernere Zukunft, durchaus wieder erzielbar.

Angesichts der nunmehr auch im österreichischen Datenschutzrecht ausdrücklich verankerten Grundsätze für die Datenqualität (Abs. 1) wird noch eine zusätzliche Bedingung für die Zulässigkeit der Verwendung von veröffentlichten Daten aufgestellt werden müssen: Gemäß § 5 Abs. 1 Z 2 dürfen Daten nur weiterverwendet werden, wenn dies mit dem ursprünglichen Ermittlungszweck nicht unververeinbar ist. Die Verwendung von veröffentlichten Daten zu einem Zweck, der dem Zweck ihrer Veröffentlichung widerspricht, müßte daher als unzulässig angesehen werden.

Die **Absätze 3 und 4** schreiben die - schon bisher unbestrittene - Auftraggeberverantwortung für Datenverarbeitungen ausdrücklich fest und führen darüber hinaus Art. 4 Abs. 2 der RL durch.

Die Richtlinie bezieht sich in Art. 27 auf sogenannte „Verhaltensregeln“, die nicht-staatliche Institutionen, wie z.B. 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 solchem „soft law“ vor allem bei der näheren Umschreibung dessen zu bestehen, was in einer bestimmten Branche als „Übung des redlichen Verkehrs“ anzusehen wäre. 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 Regeln aufgestellt würden, bedarf es allerdings einer Prüfung, die jedoch nicht von der Datenschutzkommission vorgenommen werden darf, da sonst die Unabhängigkeit der Entscheidungsfindung im einzelnen Beschwerdefall nicht gewährleistet wäre. **Absatz 5** beruft daher das für Angelegenheiten des Datenschutzes zuständige Bundeskanzleramt zu einer Begutachtung solcher Verhaltensregeln.

Zu § 6 des Entwurfs (besondere Bestimmungen für die Zulässigkeit der Ermittlung und Verarbeitung von Daten):

Die Voraussetzungen für die Zulässigkeit der Ermittlung und Verarbeitung von Daten ist, wie es der bisherigen Regelungstechnik im geltenden DSG entspricht, so vorgenommen, daß zum einen auf „ausdrückliche gesetzliche Ermächtigungen“ zur Ermittlung und Verarbeitung verwiesen wird und zum anderen eine Generalklausel für die Beurteilung der Zulässigkeit einer Datenermittlung formuliert wird. Diese Generalklausel findet sich im **Abs. 2** und stellt eine Art doppelte Bedingtheit für die Zulässigkeit der Datenermittlung und -verarbeitung auf: Es muß jeweils sowohl eine entsprechende Berechtigung des Auftraggebers vorliegen (**Z 1**) als auch die entsprechende Berücksichtigung der schutzwürdigen Interessen des Betroffenen gegeben sein (**Z 2**), damit eine konkrete Datenverarbeitung rechtmäßig ist. Auch wenn daher ein Auftraggeber an sich zur Ausübung einer bestimmten Tätigkeit berechtigt ist, ist eine konkrete Datenverwendung nur dann zulässig, wenn hiedurch überwiegende schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

Für sensible Daten gilt als Besonderheit, daß in jenen Fällen, in den eine ausdrückliche gesetzliche Ermächtigung iSd Abs. 1 nicht vorliegt, von der Generalklausel des Abs. 2 nur dann Gebrauch gemacht werden kann, wenn sich die Notwendigkeit der Verwendung sensibler Daten aus einem Gesetz ergibt. Ein solches Gesetz muß nun nicht den Determinierungsgrad einer „ausdrücklichen gesetzlichen Ermächtigung“ besitzen (- dann läge ja ein Fall des Abs. 1 vor -), vielmehr genügt ein geringerer Determinierungsgrad, für den durch den beispielhaften Verweis auf Abs. 4 oder § 41 Anhaltspunkte gegeben werden. Die ausdrückliche Erwähnung der Zulässigkeit sensibler Daten in einem solchen Gesetz ist nicht notwendig: Eine dem Abs. 2 Z 2 entsprechende Rechtsgrundlage besteht auch dann, wenn ein Gesetz eine bestimmte Tätigkeit als erlaubt vorsieht, und sich daraus zwingend ergibt, daß die Verwendung (auch) sensibler Daten notwendig ist, um eine solche Tätigkeit auszuüben. (Ein solches Gesetz ist freilich nur verfassungsmäßig, wenn es § 1 Abs. 3 entspricht.)

Abs. 3 enthält eine Sonderbestimmung für den öffentlichen Bereich, der das Legalitätsprinzip des Art. 18 B-VG nachvollzieht, wonach (- zumindest -) bei der Besorgung der Hoheitsverwaltung für jede Tätigkeit eine gesetzliche Grundlage vorhanden sein muß. Dies gilt auch für die Zulässigkeit der Vornahme von Datenverarbeitungen: Die Berechtigung hiezu ist akzessorisch zur gesetzlichen Zuständigkeit für die Vollziehung eines bestimmten Rechtsbereichs.

Abs. 4 enthält einige Fälle, in denen zweifelsfrei keine überwiegenden schutzwürdigen Geheimhaltungsinteressen des Betroffenen vorliegen. **Z 1** und **Z 2** betreffen Fälle, in welchen schon gemäß § 1 Abs. 1 das Vorliegen eines schutzwürdigen Geheimhaltungsinteresses zu verneinen ist; **Z 3** regelt einen Fall, in dem zweifelsfrei überwiegende berechtigte Interessen

eines Dritten vorliegen und **Z 4** einen Fall, in dem das überwiegende berechtigte Informationsinteresse der Öffentlichkeit an der Ausübung staatlicher Funktionen Vorrang vor den Geheimhaltungsinteressen des Betroffenen haben muß (- diese Bestimmung ersetzt die derzeit in § 3 Z 2 letzter Halbsatz DSG enthaltene Bestimmung ähnlichen Inhalts).

Abs. 5 privilegiert bestimmte Tätigkeiten von natürlichen Personen, und zwar werden private Datenverarbeitungen in die Regelungen des Entwurfs im derzeit bereits bestehenden Ausmaß einbezogen: So besteht etwa keine Registrierungspflicht und keine Informationspflicht, wohl aber z.B. das Auskunftsrecht gemäß § 23. In Abweichung von § 17 Abs. 2 DSG wird nun mehr die Terminologie der Richtlinie 95/46 verwendet, wonach von der Verwendung von Daten für „ausschließlich persönliche oder familiäre Tätigkeiten“ gesprochen wird (- auf die die Richtlinie im übrigen angesichts der Grenze des Gemeinschaftsrechts keine Anwendung findet).

Zu § 7 des Entwurfs (besondere Bestimmungen für die Zulässigkeit der Übermittlung von Daten):

Im **ersten Halbsatz des § 7 Abs. 1** ist nunmehr ausdrücklich festgeschrieben, daß derjenige, der um die Übermittlung ersucht hat, einen ausreichenden berechtigten Zweck zum Empfang dieser Daten glaubhaft machen muß.

Gegenüber den bisher in § 18 DSG enthaltenen Bedingungen einer zulässigen Übermittlung wurde insofern eine Änderung vorgenommen, als „der berechtigte Zweck des Auftraggebers“ nicht mehr als besonderer Tatbestand aufgezählt ist, der die Zulässigkeit bewirkt. Dies deshalb, weil es im Lichte des Grundrechtes auf Datenschutz keine rechtmäßige Tätigkeit geben kann, die an sich eine unbeschränkte Berechtigung zur Übermittlung personenbezogener Daten beinhaltet. Eine berechtigte Tätigkeit, die in der Übermittlung personenbezogener Daten besteht, wäre nur aufgrund eines eigenen Gesetzes denkbar, das den Bedingungen des § 1 Abs. 2 und 3 DSG entspricht und dem Verhältnismäßigkeitsprinzip entsprechende nähere Regelungen über den Grund, den Umfang und die Bedingungen für den Grundrechtseingriff enthält.

In **Abs. 2 Z 1** wird für den öffentlichen Bereich eine ausdrückliche Zulässigkeitsbestimmung für Übermittlungen festgelegt, soweit es sich um Amtshilfe im Sinne des Art. 22 B-VG handelt. Im Gegensatz zum bisherigen § 7 Abs. 2 DSG wird jedoch klargestellt, daß sie erstens nur im Bereich der Hoheitsverwaltung Geltung hat („in Vollziehung der Gesetze“) und daß sie sich nur auf die Vollziehung im Einzelfall stützen kann, was bisher zwar ständige Entscheidungspraxis war, mangels ausdrücklicher Erwähnung im Gesetz aber des öfteren zu Interpretationsschwierigkeiten geführt hat.

Zu den §§ 10 und 11 des Entwurfs (Übermittlung und Überlassung von Daten ins Ausland):

Als Ergebnis der durch die Richtlinie angestrebten - und ab 24. Oktober 1998 auch zu bewirkenden - Harmonisierung der datenschutzrechtlichen Rechtsvorschriften der EU-Mitgliedsstaaten kann - und muß - jede datenschutzrechtliche Kontrolle des Datenverkehrs zwischen EU-Staaten entfallen. Dieses Prinzip liegt **§ 10 Abs. 1** zugrunde. Dieses Prinzip gilt allerdings nicht hinsichtlich der Daten von juristischen Personen und hinsichtlich der Datenverwendung für Zwecke der sogenannten „dritten Säule“ (Zusammenarbeit der EU-Mitgliedsstaaten 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.

Über die im ersten Satz des Abs. 1 geregelten Fälle hinaus unterliegen auch die in **Abs. 3 und 4** geregelten Fälle des Datenverkehrs keinen Beschränkungen - 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 RL) oder
- wenn der Auftraggeber der Übermittlung (Überlassung) besondere Garantien für die Gewährleistung der Betroffenenrechte im Ausland bietet (Art. 26 Abs. 2 RL).

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 § 10 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-Mitgliedsstaaten betreffend juristische Personen und die sog. „dritte Säule“ zulässig). In allen anderen Fällen muß die Beurteilung von Fall zu Fall geschehen, und zwar anläßlich des Genehmigungsverfahrens gemäß § 11 (Art. 25 Abs. 2 der RL).
Die zum Zweck einer einheitlichen Beurteilung dieser Fragen in allen EU-Mitgliedsstaaten vorgesehenen Mitteilungs- und Durchführungspflichten sind in den §§ 50 und 51 umgesetzt.

Zu § 12 des Entwurfes (Datensicherheitsmaßnahmen):

Die bisherigen Erfahrungen lassen es sinnvoll erscheinen, genauere Bestimmungen über Protokoll- und Dokumentationsdaten in das DSG aufzunehmen.

Die Schaffung einer besonderen Verantwortlichkeit für Datenverarbeitungen, die der Vorabkontrolle unterworfen sind, ist ein geeignetes Mittel, um die ordnungsgemäße Durchführung solcher Verarbeitungen, die für die Geheimhaltungsinteressen besonders relevant sind, zu gewährleisten.

Zu § 13 des Entwurfes (Datengeheimnis):

Die Verpflichtung von Mitarbeitern (**Abs. 1**) eines Auftraggebers oder Dienstleisters zur Geheimhaltung von Daten, die ihnen aufgrund 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 anordnenden Organen des Auftraggebers oder Dienstleisters und durchführenden Mitarbeitern deutlicher zum Ausdruck bringen, was insbesondere auch im Hinblick auf die neu formulierten Verwaltungsstrafbestimmungen in § 48 notwendig war.

Zu § 14 des Entwurfs (Datenverarbeitungsregister):

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

- die Meldung von Datenverarbeitungen an ein Register, das von der unabhängigen Kontrollstelle (Art. 28 der RL) zu führen ist,
- die Bestellung eines internen Datenschutzbeauftragten, der eine Liste der Datenverarbeitungen des Auftraggebers zu führen hat,
- 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 des Registers der Datenverarbeitungen Gebrauch; dieses ist in Hinkunft richtlinienkonform von der Datenschutzkommission zu führen.

Zu § 15 des Entwurfs (Meldepflicht):

Entsprechend der Richtlinie 95/46/EG sind Verarbeitungen, die „spezifische Risiken für die Rechte und Freiheiten von Personen beinhalten können“, einer sogenannten „Vorabkontrolle“ zu unterwerfen, d.h. daß sie vor ihrer Aufnahme durch die unabhängige Kontrollinstanz auf ihre Rechtmäßigkeit zu prüfen sind. Dementsprechend ist in **Abs. 2** festgelegt, welche Kategorien von Datenverarbeitungen 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. Alle anderen Datenverarbeitungen dürfen - soweit sie überhaupt meldepflichtig sind - sofort nach der Meldung aufgenommen werden. Bezüglich der von Abs. 2 nicht erfaßten Datenverarbeitungen ändert sich materiell somit nichts gegenüber der bisherigen Rechtslage.

Bei richtlinienkonformer Definition der automationsunterstützten Datenverarbeitung sind auch nicht-strukturierte elektronische Datensammlungen - im Gegensatz zur bisherigen Rechtslage in Österreich - unter den Begriff der Datenverarbeitung zu subsumieren. Daher sind einer Datenverarbeitung iSd § 3 Z 7 auch jene Datenverwendungsschritte hinzuzurechnen, die nicht-strukturierte Texte erzeugen oder speichern, aus welchen sich der Inhalt jener Daten ergibt, die im strukturierten Teil der Datenverarbeitung als aufbereitete Information gespeichert sind. Eine gesonderte Registrierung der nicht-strukturierten Teile einer Datenverarbeitung ist daher gemäß **Abs. 3** nicht vorgesehen.

Die Beurteilungskriterien des Art. 18 Abs. 2 RL gelten auch für die Möglichkeit, Datenverarbeitungen von der Registrierungspflicht auszunehmen, was in **§ 15 Abs. 4** geschieht:
Die wichtigste Ausnahme sind die sogenannten „Standardverarbeitungen“ (**Z 4**), deren Zulässigkeitsvoraussetzungen allerdings etwas geändert werden mußten, um richtlinienkonform zu sein. Die meisten der heute bestehenden Standardverarbeitungen werden dennoch auch unter der neuen Rechtslage als - nicht meldepflichtige - Standardverarbeitungen aufrecht erhalten werden können.
Die Ausnahmen von der Registrierungspflicht für „persönliche“ Datenverarbeitungen (**Z 1**) kann richtlinienkonform vorgenommen werden, weil diese Verarbeitungen nicht in den Anwendungsbereich der Richtlinie fallen. Was die Ausnahme für die Führung gesetzlich eingerichteter öffentlicher Register betrifft (**Z 3**), ist diese in der Richtlinie selbst vorgesehen (Art. 21 Abs. 3 zweiter Unterabsatz). Der Entfall der Registrierungspflicht nach **Z 2** ergibt sich schließlich daraus, daß die bloße Kenntnisnahme veröffentlichter Daten kein schutzwürdiges Geheimhaltungsinteresse berührt (vgl. § 1 Abs. 1) und außerdem jedermann im Rahmen des Grundrechts auf Meinungsäußerungsfreiheit (Art. 10 MRK), das auch das Recht zum Empfang von Nachrichten verbürgt, freisteht, sodaß es nicht der in der Registrierung zu sehenden Beschränkung unterworfen werden darf.

Die bisherigen Regelungen in § 4 Abs. 3 DSG über Datenverarbeitungen, für die im Interesse der Staatssicherheit das Publizitätsprinzip nicht gelten soll, waren weder zufriedenstellend noch effektiv. Das nunmehr in **Abs. 5** vorgeschlagene Regelungssystem enthält eine Verpflichtung zur Offenlegung von Datenverarbeitungen gegenüber der Datenschutzkommission, allerdings verbunden mit der Möglichkeit, die Veröffentlichung durch Eintragung in das Datenverarbeitungsregister zu unterlassen. Entspricht die Datenschutzkommission einem diesbezüglichen Antrag eines Auftraggebers des öffentlichen Bereichs nicht, besteht die Möglichkeit einer Amtsbeschwerde gemäß § 36 Abs. 3.

Zu § 16 des Entwurfes (Inhalt der Meldung):

Neu ist hinsichtlich des Inhalts von Meldungen nur **Z 7**, wonach - in Erfüllung der Erfordernisse der Richtlinie 95/46/EG - allgemeine Angaben über die im konkreten Fall bestehenden Datensicherheitsmaßnahmen zu machen sind. Zu denken wäre hier an Aussagen darüber, ob die gemäß § 12 Abs. 2 oder auch Abs. 5 erforderlichen Maßnahmen ergriffen wurden, oder welche Ziffern des § 12 Abs. 2 nicht umzusetzen waren, weil dies im Lichte des § 12 Abs. 1 nicht erforderlich ist.

Im öffentlichen Bereich sind gelegentlich Datenverarbeitungen aufgrund derselben gesetzlichen Bestimmungen und daher mit demselben Inhalt von vielen Auftraggebern in gleicher Weise durchzuführen. Manche diese Datenverarbeitungen kommen wegen ihres Zwecks oder wegen der verarbeiteten Datenarten für eine Erklärung zur Standardverarbeitung nicht in Frage. Dennoch kann die Festlegung ihres genauen Inhalts durch Verordnung sinnvoll sein, da hiedurch eine bindende Interpretation über den zulässigen Inhalt der Datenverarbeitung erfolgt, was einen geringeren Vollziehungsaufwand auf seiten der Auftraggeber bedeutet, aber auch eindeutig im Interesse der Betroffenen liegt, da ein höheres Ausmaß an Rechtssicherheit gewährleistet wird.
Die Meldung solcher Datenverarbeitungen in der in § 16 Abs. 2 vorgesehenen Form stellt keine Vereinfachung der Meldung iSd Art. 18 Abs. 2 der Richtlinie dar, da der gesamte von Art. 19 der Richtlinie geforderte Inhalt der Datenverarbeitung eindeutig offengelegt wird: Die Auftraggeber einer solchen Datenverarbeitung haben in ihrer Datenverarbeitung genau den von den Verordnungen definierten Inhalt zu verwirklichen - dies ergibt sich aus dem Legalitätsprinzip der öffentlichen Verwaltung und der Verbindlichkeit der Musterverordnung.

Zu § 19 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 § 19 Abs. 3 in Verbindung mit § 34 Abs. 1 wird für diese Richtigstellungen eine Art von „Einzelrichterentscheidung“ in einem Mandatsverfahren geschaffen mit der Möglichkeit, Vorstellungen an das Plenum der Datenschutzkommission zu erheben. Die weitere Anrufbarkeit des Verwaltungsgerichtshofes ist gemäß § 36 Abs. 1 ausgeschlossen, da bei der vorliegenden Konstellation ein Abgehen von Art. 133 Z 4 B-VG nicht geboten erscheint.

Zu § 20 des Entwurfs (Offenlegung nicht meldepflichtiger Datenverarbeitungen):

Die Richtlinie 95/46/EG schreibt in Art. 21 Abs. 3 bei Datenverarbeitungen, 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 Standardverarbeitungen: Dies deshalb, weil Datenverarbeitungen für den persönlichen oder familiären Bereich (§ 15 Abs. 4 Z 1) außerhalb des Geltungsbereiches der Richtlinie liegen, sodaß diesbezüglich keine Offenlegungspflicht besteht (- im übrigen besteht hinsichtlich dieser Verarbeitungen das Auskunftsrecht des Betroffenen gemäß § 23); gesetzlich vorgesehene öffentliche Register (**Z 3**) dürfen gemäß ausdrücklicher Bestimmung der Richtlinie (Art. 21 Abs. 3) ausgenommen werden - die Existenz dieser Register ergibt sich schon aus gesetzlichen Vorschriften; die bloße Abfrage (also Kenntnisnahme) von öffentlichen Datensammlungen bedarf deshalb keiner eigenen Offenlegung, weil schutzwürdige Geheimhaltungsinteressen der Betroffenen nicht berührt werden (vgl. dazu die Ausführungen zu § 1 Abs. 1; letztere Ausnahme ist auch kein Widerspruch zur Richtlinie: vgl. dazu die Ausführungen zu § 5 Abs. 2 und § 15 Abs. 4).

Zu § 21 des Entwurfs (Informationspflicht des Auftraggebers):

Dies ist eine der wesentlichsten Neuerungen der Richtlinie gegenüber der bisherigen österreichischen Rechtslage. Sie soll es dem Betroffenen zusätzlich erleichtern, seine Rechte zu wahren. Daß nur meldepflichtige Datenverarbeitungen der Informationspflicht unterliegen, geht aus der Natur der gemäß § 15 Abs. 4 nicht meldepflichtigen Fälle hervor:

- Für Verarbeitungen zu persönlichen und familiären Zwecken gilt die Richtlinie nicht und daher auch nicht 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 klar 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“;
- was die bloße Abfrage aus öffentlichen Datensammlungen betrifft, ist aus der „Öffentlichkeit“ des Zugangs zu diesen Daten abzuleiten, daß der Betroffene mit der Kenntnisnahme dieser Daten durch jedermann rechnen muß, sodaß eine besondere Informationspflicht unverhältnismäßig wäre (vgl. auch die Ausführungen zu § 15 Abs. 4).

Zu § 22 des Entwurfs (Offenlegung der Identität des Auftraggebers):

Die bisherigen Erfahrungen haben gezeigt, daß die Verfolgung von Betroffenenrechten dann sehr schwierig ist, wenn Daten eines Auftraggebers - z.B. 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 keine Widerspruchs- bzw. Löschungsrechte geltend machen. Diesem Problem soll § 22 abhelfen.

Zu § 23 des Entwurfes (Auskunftsrecht):

Im neuen § 23 sind die bisher geltenden §§ 11 und 25 zusammengefaßt. Hinsichtlich des Regelungsinhalts wurden im wesentlichen nur Korrekturen zum Zweck der Klarstellung vorgenommen. **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.

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 Datenverarbeitungen des Auftraggebers vorhanden sein könnte, eine beträchtliche Belastung des Auftraggebers (u.U. 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. 4, daß Auskunft dann unentgeltlich zu erteilen ist, wenn die Auffindung der zu beauskunftenden Daten für den Auftraggeber keine besondere Belastung darstellt („wenn sie Dateien betrifft, die beim Auftraggeber in direktem Zugriff stehen“). In allen anderen Fällen ist Auskunft kostenpflichtig, wobei ein niedriger Grundtarif im Gesetz festgelegt ist, von dem in begründeten Fällen abgewichen werden darf. Ob derartige Abweichungen gerechtfertigt sind, wäre in einem Verfahren vor der Datenschutzkommission gemäß § 27 Abs. 1 überprüfbar.

Wird ein Auskunftsbegehren an einen Auftraggeber gestellt, so muß dieser zumindest Antwort dahin geben, warum er eine Auskunft zur Gänze oder teilweise nicht erteilt. Um diese

Antwortverpflichtung besser durchzusetzen, wurde im § 48 Abs. 1 Z 8 eine eigene Verwaltungsstrafbestimmung geschaffen. Diese besteht unabhängig davon, ob in der Folge ein Verfahren gemäß § 27 Abs. 1 auf Antrag des Betroffenen eingeleitet wird oder nicht.

Zu § 24 des Entwurfs (Recht auf Richtigstellung oder Löschung):

§ 24 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 **§ 24 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. 2 trägt dem Umstand Rechnung, daß manche Datenverarbeitungen 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 (z.B. bei der Führung von Krankengeschichten).

Zu § 25 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 der Datenverarbeitung, gegenüber der das Widerspruchsrecht geltend macht, gelöscht werde.

Die Statuierung eines solchen Widerspruchsrechtes ist aus der Sicht des österreichischen DSG nur scheinbar eine Neuerung: Da für die Beurteilung der Zulässigkeit einer Ermittlung und Verarbeitung von Daten eine Interessensabwägung dahingehend notwendig ist, ob nicht überwiegende berechtigte Interessen des Betroffenen verletzt sind, ist das Widerspruchsrecht nichts anderes als die Beschwerde des Betroffenen, daß in seinem Fall die Interessensabwägung falsch vorgenommen wurde. Insofern war diese Konstellation auch bisher durch das Beschwerderecht nach § 14 DSG abgedeckt. Gegenüber einer Datenverarbei-

tung, die die Betroffenenkreise gesetzlich festlegt, kann ein Widerspruchsrecht freilich nicht geltend gemacht werden, da in diesem Fall die Interessensabwägung abschließend durch Gesetz vorgenommen wurde. (Allenfalls kann hier die Überprüfung der gesetzlichen Bestimmung auf ihre Verfassungsmäßigkeit im Lichte des § 1 DSG angestrebt werden).

In **Abs. 2** wird eine zusätzliche Spielart des Widerspruchsrechts ausdrücklich geregelt, die in der Praxis nach den bisherigen Erfahrungen sehr 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 ein schutzwürdiges Interesse an der Geheimhaltung von Daten infolge des Zwecks der Datenverarbeitung und der verwendeten Datenarten nicht besteht. Beispielsfälle wären etwa Verzeichnisse österreichischer Gewerbetreibender, die für Exportförderungszwecke verwendet werden; Einwohnerverzeichnisse; Verzeichnisse von Fernsprechteilnehmern, Telefaxanschlüssen, E-Mail-Adressen, etc. Derartige öffentlich zugängliche Verzeichnisse ruhen zum größten Teil nicht auf ausdrücklichen gesetzlichen Regelungen. Um einen fairen Interessensausgleich zu gewährleisten, scheint es sinnvoll, Personen, die in Abweichung von der durchschnittlichen Einschätzung ihrer Geheimhaltungsinteressen ein überwiegendes Interesse daran behaupten, daß sie in diesen Verzeichnissen nicht aufscheinen, ein Widerspruchsrecht gegen die Aufnahme in solche Verzeichnisse einzuräumen. Hiedurch 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. Diese Regelung findet in Art. 14 lit. a der Richtlinie ebenfalls ihre Deckung, da es sich auch hier um die Geltendmachung von überwiegenden schutzwürdigen Geheimhaltungsinteressen geht, die sich aus der besonderen Situation des Betroffenen ergeben.

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 § 26 des Entwurfs (Kontrollbefugnisse der Datenschutzkommission):

Die Richtlinie 95/46/EG mißt der Kontrolle von Datenverarbeitungen 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 beinhaltet das Recht, Einschau in Datenverarbeitungen und Unterlagen zu nehmen, Auskünfte zu verlangen, dem Auftraggeber Empfehlungen und Ermahnungen zu erteilen und kann bis zu einem gewissen Grad auch rechtsförmliche Akte umfassen, soweit z.B.

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 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 ohne einen solchen Anlaß. Rechtsförmliche Entscheidungen über behauptete Datenschutzverletzungen werden hingegen so wie bisher von der Datenschutzkommission zu treffen sein, wenn sie Auftraggeber des öffentlichen Bereichs betreffen, und von den ordentlichen Gerichten, wenn sie Auftraggeber des privaten Bereichs betreffen.

Die Konsequenzen einer Nichtbefolgung einer Empfehlung der Kontrollstelle sind in Abs. 3 näher geregelt, wobei darauf hinzuweisen ist, daß Z 4 die bisherigen Bestimmungen des § 41 DSG ersetzt.

Die Kontrollbefugnisse der unabhängigen Kontrollstelle (in Österreich: Datenschutzkommission) beziehen sich auf alle Datenverarbeitungen auf österreichischem Hoheitsgebiet und werden durch die allfällige Anwendbarkeit der Rechtsordnung eines anderen EU-Mitgliedstaates gemäß § 2 nicht beschränkt. Um die daraus resultierenden Probleme zu reduzieren, ist die gegenseitige Hilfeleistung der Kontrollstellen auch im österreichischen Datenschutzgesetz ausdrücklich festgeschrieben (Abs. 4 und 5).

Zu § 27 des Entwurfs (Beschwerde an die Datenschutzkommission):

Die Datenschutzkommission übt neben ihrer Kontrollfunktion auch eine quasi-richterliche Entscheidungfunktion 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 Zuständigkeit für behauptete Verletzungen des Auskunftsrechtes, 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.

Zu § 28 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 immer die Datenschutzkommission zuständig ist. 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 erheben kann zur Feststellung der Rechtmäßigkeit einer Datenverwendung. Diese Möglichkeit ist auf vermutete schwerwiegende Datenschutzverletzungen beschränkt und soll für solche Fälle, an deren Klärung 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. Was die Möglichkeit einer Nebenintervention gemäß § 17ff ZPO betrifft, haben die bisherigen Erfahrungen gezeigt, daß es zielführender ist, hier keine zwingende Bestimmung für das Einschreiten der Datenschutzkommission vorzusehen, sondern dies dem pflichtgemäßen Ermessen der Datenschutzkommission zu überlassen.

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

Zu § 29 des Entwurfs (Schadenersatz):

In Umsetzung von Art. 23 Abs. 1 der Richtlinie enthält § 29 nunmehr ausdrückliche Bestimmung über den Ersatz erlittenen Schadens. Dafür gelten zunächst die allgemeinen Bestimmungen des Schadenersatzrechts; gehaftet wird nur bei Verschulden. Für besonders schwerwiegende Fälle rechtswidriger Datenverwendung sieht Abs. 3 den Ersatz immaterieller Schäden vor, wobei die Entschädigung in Anlehnung an die vergleichbaren Bestimmungen des Mediengesetzes mit S 200.000,-- begrenzt ist. Fälle besonders schwerwiegender Datenschutzverletzungen werden in Abs. 3 beispielhaft aufgezählt; hiebei ist neben der feh-

lerhaften insbesondere auch die rechtsmißbräuchliche Datenverwendung Regelungsgegenstand.

Nach dem Abs. 2 trifft die schadenersatzrechtliche Haftung nur den Auftraggeber und den Dienstleister; dahinter steht die Überlegung, daß es für den Betroffenen schwer erkennbar ist, welche konkrete Person im Verantwortungsbereich des Auftraggebers oder Dienstleisters den Schaden verschuldet hat. Es soll verhindert werden, daß der Auftraggeber oder Dienstleister die Geltendmachung von Ersatzansprüchen dadurch erschwert, daß er es unterläßt, zur Ermittlung des Schädigers beizutragen. Auftraggeber und Dienstleister sollen zur ungeteilten Hand haften (**Abs. 3**).

Verletzungen von Datenschutzbestimmungen erfolgen häufig außerhalb von Vertragsverhältnissen zum Geschädigten, sodaß die Regelung des § 1313a ABGB nicht zur Anwendung kommt. Aus der bereits angesprochenen mangelnden Nachvollziehbarkeit der Datenverarbeitungsvorgänge für den Betroffenen erscheint es sachgemäß, dem Auftraggeber bzw. Dienstleister das Verhalten seiner Leute zuzurechnen und die Haftung bei ihm zu konzentrieren. **Abs. 4** übernimmt daher die Regelung des § 1313a ABGB sinngemäß für sämtliche Haftungen aus rechtswidrigen Datenverwendungen.
Die in **Abs. 2** 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 § 31 des Entwurfs:

§ 31 stellt eine Zusammenfassung und verfassungsrechtliche Absicherung der Zuständigkeiten der Datenschutzkommission dar. 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 der 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 die Ausführungen zu § 48 Abs. 5 sowie das Urteil des EGNR im Fall Bönisch gg. Ö.; EuGRZ 1986/127).

Zu § 36 des Entwurfes (Wirkung von Bescheiden der Datenschutzkommission):

Für die im Registrierungsverfahren ergehenden Mandatsbescheide besteht das Rechtsmittel der Vorstellung an die Datenschutzkommission. Eine Anrufungsmöglichkeit des Verwaltungsgerichtshofes in Abgehen von der Bestimmung des Art. 133 Z 4 B-VG schien daher nicht sachlich geboten.

Hinsichtlich der anderen bescheidmäßigen Erledigungen der Datenschutzkommission besteht die generelle Möglichkeit, den Verwaltungsgerichtshof anzurufen, nur für die Parteien des Verfahrens, nicht aber für die belangte Behörde. Soweit Auftraggeber des öffentlichen Bereichs selbst Antragsteller im Verfahren vor der Datenschutzkommission sind, nämlich im Registrierungs- und im Genehmigungsverfahren, wird ihnen durch Abs. 3 die Möglichkeit einer Amtsbeschwerde eröffnet.

Zu § 41 des Entwurfs (Sensible Daten):

Wie schon in den Ausführungen zu § 1 Abs. 3 erwähnt, sind jene Tatbestände des Art. 8 der Richtlinie, die die Verarbeitung sensibler Datenarten in bestimmten Fällen wegen überwiegender Rechte und Freiheiten Dritter zulassen, in § 41 konzentriert. Da § 1 Abs. 3 als Zulässigkeitsvoraussetzung für die Verwendung sensibler Daten das Vorliegen wichtiger öffentlicher Interessen verlangt, muß § 41 im Verfassungsrang beschlossen werden, um einen Normen-Widerspruch auf unterschiedlichen Rechtsstufen zu vermeiden. Durch die vorgeschlagene Regelungstechnik wird erreicht, daß die Verwendung sensibler Daten in den von der Richtlinie vorgesehenen Fällen auch nach österreichischem Recht erlaubt ist, daß aber außerhalb des DSG durch einfache Gesetze die Verwendung sensibler Daten nur aus „wichtigen öffentlichen Interessen“ angeordnet werden darf.

Zu § 42 des Entwurfs (Daten über Verurteilungen):

Daten, die Straftaten, strafrechtliche Verurteilung und vorbeugende Maßnahmen betreffen, sind in der Richtlinie zwar nicht in den taxativen Katalog der sensiblen Daten (Art. 8 Abs. 1 RL) aufgenommen, werden aber in unmittelbarer Nähe zu den sensiblen Daten geregelt, nämlich in Art. 8 Abs. 5 RL. Es liegt auch auf der Hand, daß Daten mit diesem Inhalt für den Betroffenen besonders nachteilig verwendet werden können und daher ebenso sensibel wie die in Art. 8 Abs. 1 RL enthaltenen Daten sind. Dementsprechend sieht § 42 vor, daß die Verwendung der genannten Datenarten in Datenverarbeitungen nur dann zulässig ist, wenn dies in einem Gesetz ausdrücklich vorgesehen ist. Diese Bestimmung ist besonders wichtig gegenüber dem in letzter Zeit zunehmenden Trend, branchenspezifische Informationsverbundsysteme über strafrechtlich relevante Daten von Kunden und Interessenten zu schaffen,

wobei vielfach auch der bloße Verdacht eines strafrechtlich relevanten Sachverhalts für die Eintragung in ein solches System genügt. Daß hier zum Schutz des Betroffenen ausdrückliche Regelungen über den Anlaß und die näheren Umstände der Eintragung in ein solches Informationsverbundsystem notwendig sind, ist evident.

Zu § 43 des Entwurfs (Adreßdaten):

Diese Bestimmung wurde aufgrund der bisherigen Erfahrungen geschaffen, wonach sich ergeben hat, daß dieses Problem ohne ausdrückliche gesetzliche Regelung unlösbar ist. Wiederholt wurde das Bundeskanzleramt mit dem Problem befaßt, das bestimmte Betroffenenkreise über Dinge, die für sie wichtig sind, informiert werden sollten, die Identifikationsdaten dieser Betroffenenkreise jedoch von jenen Stellen, die sie aufgrund anderer Datenverarbeitungen 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 Identifikationsdaten von bestimmten Betroffenenkreisen benötigt werden, um mit ihnen in Kontakt zu treten. Um in dieser Situation berechtigten Informationsinteressen einerseits und möglicherweise bestehenden Geheimhaltungsinteressen andererseits gerecht zu werden, wird die Datenschutzkommission mit der Aufgabe betraut, im einzelnen Fall zu prüfen, ob eine konkrete Übermittlung von Adreßdaten eines bestimmten Betroffenenkreises die schutzwürdigen Geheimhaltungsinteressen der Betroffenen gefährden würde oder ob das Interesse der Betroffenen oder ein öffentliches Interesse an der Ermöglichung der Kontaktaufnahme mit den Betroffenen überwiegt.

Zu § 44 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, z.B. 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 Zulässigkeitsvoraussetzungen für die 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.

In allen anderen Bereichen findet die Richtlinie unbeschränkte Anwendung auf publizistische Tätigkeit, das sind

- Kapitel I: Allgemeine Bestimmungen über die Anwendung der innerstaatlichen Rechtsordnung sowie Definitionen datenschutzrechtlich relevanter Begriffe,
- Kapitel III: Rechtsbehelfe, Haftung und Sanktionen,
- Kapitel V: branchenspezifische Verhaltensregeln
- (Kapitel VII: gemeinschaftliche Durchführungsmaßnahmen; dies bedarf keiner gesonderten Umsetzung der Richtlinie im vorliegenden Zusammenhang).

Vor diesem Hintergrund sind die lapidaren Bemerkungen des § 54 DSG über „Ausnahmen für Medienunternehmen“ nicht mehr ausreichend. Es muß vielmehr ausdrücklich dargelegt werden, inwieweit die österreichische Rechtslage Ausnahmen voraussieht, die im Lichte der Richtlinie zulässig sind.

Hiezu ist zunächst eine terminologische Bemerkung zu machen: Die Richtlinie spricht von „journalistischen Tätigkeiten“, ohne hiefür eine Definition zu geben. Aus dem Zweck des Art. 9 RL 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.
Betreffend die notwendigen - und zulässigen - Ausnahmen für diese Tätigkeit ist folgendes zu sagen:
Auf die publizistische Tätigkeit im Sinne des § 44 Abs. 1 finden richtlinienkonform Anwendung:

- die §§ 2 bis 4 des Entwurfes (entspricht dem Kapitel I der Richtlinie)

- die Bestimmungen des 3. Abschnitts des Mediengesetzes über Rechtsbehelfe, Haftung und Sanktionen (entspricht dem Kapitel III der Richtlinie)
- § 5 Abs. 5 über die Zulässigkeit und Bedeutung branchenspezifischer Verhaltensregeln (Kapitel V der Richtlinie).

Ausnahmen bestehen von den Kapiteln II, IV und VI in folgendem Umfang:
Ausnahmen von Kapitel II der Richtlinie:

1. Es gelten die Grundsätze über die Datenqualität (Art. 6 der Richtlinie, § 5 Abs. 1 DSG-Entwurf).
2. Für die Zulässigkeit der Datenverwendung gelten die besonderen Bestimmungen des § 44 Abs. 2 des Entwurfs, ergänzt durch das Mediengesetz hinsichtlich der Zulässigkeit von Veröffentlichungen.
3. Die Betroffenenrechte können, soweit sie die unmittelbaren Grundlagen (Datensammlungen) einer journalistisch/publizistischen Veröffentlichung betreffen, nicht ausgeübt werden.
   „Für den Schutz der Meinungsäußerungsfreiheit ist es beispielsweise wesentlich, daß geplante Veröffentlichungen nicht durch eine vorzeitige Intervention - sei es durch betroffene Personen, sei es durch die Kontrollstelle - gestört oder vereitelt werden." (Dammann/Simitis, EG-Datenschutzrichtlinie, Kommentar, S. 177). Dies gilt freilich nicht für jene Datensammlungen, die nicht unmittelbar einer Veröffentlichung im Sinne des Mediengesetzes dienen, sondern als allgemein zugängliche Informationsdienste jedermann - wenn auch gegen Entgelt - zur Verfügung stehen: „In bezug auf bereits veröffentlichtes Material besteht keine (dem obigen Zitat) vergleichbare Gefährdung" (Dammann/Simitis, a.a.O.).
4. Die Bestimmungen über Datensicherheitsmaßnahmen sind zur Gänze anzuwenden (Art. 16 und 17 der Richtlinie, §§ 12 und 13 des DSG-Entwurfes).
5. Die Bestimmungen über die Publizität von Datenverarbeitungen finden aus denselben Gründen und im selben Umfang wie unter 3. dargelegt, keine Anwendung.

Ausnahmen von Kapitel IV der Richtlinie:
Eine Genehmigungspflicht für die grenzüberschreitende Veröffentlichung in Medien wäre in Österreich verfassungswidrig, da dies eine Art von Vorzensur darstellen würde. Vollständigkeitshalber sei erwähnt, daß hinsichtlich des Datenexports aus Datensammlungen, die nicht unmittelbar einer publizistischen Tätigkeit dienen, im übrigen dann Genehmigungsfreiheit gemäß § 3 Z 3 gilt, wenn sie im Inland bereits „veröffentlicht", d.h. allgemein zugänglich sind. Dies wird bei den Informationsdatenbanken der Mediendienste regelmäßig der Fall sein.

Ausnahmen von Kapitel VI der Richtlinie:
Aus den unter Punkt 3 zu Kapitel II erwähnten Gründen kann eine Kontrolle in der im DSG-Entwurf vorgesehenen Form gegenüber dem Kernbereich publizistischer Tätigkeit nicht er-

folgen. Diesbezüglich gelten die Bestimmungen des Mediengesetzes, das - ausschließlich in Form einer ex-post-Kontrolle - umfangreiche und spezifische Mittel der Rechtsverfolgung durch den Betroffenen enthält. Als zusätzliches Mittel der Kontrolle im Medienbereich sei auch die auf Verhaltensregeln iSd § 5 Abs. 5 beruhende Tätigkeit des Presserates erwähnt.

Zu § 46 (Informationsverbundsysteme):

Zum Zweck eines besseren Service für die Betroffenen (z.B. 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 System-Teilnehmer 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 ernsthaft bezweifelt werden muß. Für jene Informationsverbundsysteme, die ihrem Zweck nach eine Kontrolle über den Betroffenen ausüben sollen (z.B. über seine Kreditwürdigkeit, seine Aufenthaltsberechtigung in einem bestimmten Territorium etc.), ist daher nunmehr ein absoluter Gesetzesvorbehalt eingeführt: Um zu gewährleisten, daß solche Informationsverbundsysteme nur eingerichtet werden, wenn hiefür ein überwiegendes, in einer demokratischen Gesellschaft gerechtfertigtes Interesse besteht, und daß nur die unbedingt notwendigen Informationen mit möglichst hoher Datenqualität (insbesondere Richtigkeit und Vollständigkeit der Daten) und nur bei vorher definierten Anlässen gespeichert werden, muß eine ausdrückliche gesetzliche Regelung für jedes einzelne dieser Informationsverbundsysteme erfolgen.

Der Umstand, daß dem Betroffenen bei einem Informationsverbundsystem eine Vielzahl von Auftraggebern gegenüber steht, ist für die Ausübung seiner Betroffenenrechte (§§ 23 bis 25 des Entwurfes) nachteilig. Deshalb wird nunmehr die Bestellung eines „Betreibers“ zwingend vorgeschrieben, der der Ansprechpartner des Betroffenen und ihm gegenüber Quasi-Auftraggeber ist. (Art. 2 lit. d der Richtlinie eröffnet die Möglichkeit einer solchen vom Normalfall abweichenden Regelung).

Das Innenverhältnis zwischen dem Betreiber und den Auftraggebern bleibt der vertraglichen Ausgestaltung überlassen, mit Ausnahme von zwei Punkten:

1. der Betreiber hat gegenüber den Betroffenen (also nicht etwa in Strafverfahren) alle Auftraggeberpflichten wahrzunehmen;
2. der Betreiber ist für die EDV-organisatorische und EDV-technische Seite der Datenaufbereitung im System verantwortlich. Dies ist wesentlich für eine möglichst hohe Datenquali-

tät in einem Informationsverbundsystem. Das hohe Gefährdungspotential eines Informationssystems mit Kontrollfunktion muß optimale Datenqualität gewährleisten, damit es nicht zum unverhältnismäßigen und daher unzulässigen Eingriff in das Grundrecht auf Datenschutz wird.

Zu den §§ 47 und 48 des Entwurfs (Strafbestimmungen):

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 eines besonderen Berufsgeheimnisses in der vorliegenden Form als sachgerecht angesehen werden konnte. Diese Voraussetzung hat sich völlig verändert: Angesichts des Umstandes, daß die meisten beruflichen Tätigkeiten in der einen oder anderen Form mit der Benutzung von Datenendgeräten verbunden ist, sodaß nahezu jedermann in seiner beruflichen Tätigkeit (auch) mit „Aufgaben der Datenverarbeitung“ betraut ist, kann von dem ursprünglich beabsichtigten besonderen Berufsgeheimnis keine Rede mehr sein: Dieses Tatbestandselement wird im Prinzip bei jedermann zutreffen. Eine solche Ausweitung des potentiellen Täterkreises führt zu einem Kriminalisierungspotential, das ursprünglich nie beabsichtigt war. Hiezu kommt, daß der Tatbestand insgesamt wenig spezifisch formuliert ist, sodaß nahezu jede Indiskretion in bezug auf personenbezogene Daten, die aus einer beruflichen Tätigkeit resultiert, gerichtlich strafbar 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 § 48 ein Tatbestand aufgenommen, der an die Verletzung des Datengeheimnisses (§ 13 des Entwurfes) anknüpft (nähere Ausführungen siehe unten).

Gerichtlich strafbar verbleibt jedoch wegen seiner besonderen Verwerflichkeit der Tatbestand, daß jemand sich Daten in Schädigungsabsicht beschafft. Um allerdings das Gleichgewicht zu vergleichbaren Tatbeständen des StGB herzustellen, wurde im vorliegenden Entwurf die Verfolgbarkeit an die Ermächtigung des Verletzten oder einen Antrag der Datenschutzkommission gebunden.

Was nun die in § 48 Abs. 1 vorgesehenen Verwaltungsstraftatbestände betrifft, wurde vom Grundsatz ausgegangen, daß ein Verwaltungsstraftatbestand dort eingeführt wird, wo man-

gels subjektiver Rechte des Betroffenen eine Rechtsverfolgung seinerseits nicht möglich ist. Derartige Ordnungswidrigkeiten müssen daher auf anderem Wege, nämlich im Wege von Verwaltungsstrafbestimmungen, geahndet werden.

Die **Z 1 und 2** des § 48 Abs. 1 betreffen Verletzungen des Datengeheimnisses, und zwar direkt (Z 2) oder indirekt durch Erlassung rechtswidriger Anordnungen (Z 1). **Z 3** sanktioniert das Verharren im rechtswidrigen Zustand, wenn nämlich durch Urteil oder Bescheid der rechtmäßige Zustand bereits festgestellt ist bzw. seine Herstellung angeordnet wurde, der Verpflichtete diesem Urteil oder Bescheid jedoch nicht entspricht. Die Meldepflicht und die Pflicht zur Einholung einer Genehmigung für den Datenexport ins Ausland sind schließlich Verpflichtungen des Auftraggebers, denen kein subjektives Recht des Betroffenen gegenübersteht; ihre Verletzung wird daher so, wie schon bisher im DSG, durch Verwaltungsstrafe geahndet (**Z 4 und 5**). Desgleichen sind die Pflichten der §§ 20, 21 und 22 nicht als subjektives Recht des Betroffenen konstruiert, weshalb auch diesbezüglich eine Verwaltungsstrafe bei Verletzung vorgesehen werden mußte (**Z 7**). Der Tatbestand der **Z 8** soll schließlich in besserem Ausmaß als bisher gewährleisten, daß Auftraggeber einem Auskunftsantrag eines Betroffenen - zumindest durch Beantwortung - entsprechen.

Bisher war die Frage, ob Auftraggeber des öffentlichen Bereichs den bereits vorhandenen Verwaltungsstraftatbestimmungen des § 50 DSG unterliegen können, nicht zweifelsfrei geklärt. Der ausdrücklichen Regelung dieser Frage dient **Abs. 2**, der im Interesse des Sachlichkeitsgebotes die anordnungsbefugten Organe von Auftraggebern des öffentlichen Bereichs hinsichtlich ihrer verwaltungsstrafrechtlichen Verantwortung den Organen von Auftraggebern des privaten Bereichs gleichstellt.

Bisher waren die Landeshauptleute in erster Instanz als Strafbehörde zuständig. Vertreter der Länder haben demgegenüber ins Treffen geführt, daß aufgrund der derzeit vorherrschenden Zuständigkeitsverteilung den Ämtern der Landesregierung 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. 5 nunmehr geschieht. Hinsichtlich des Umstandes, daß in zweiter Instanz nicht mehr die Datenschutzkommission tätig werden soll, vgl. dazu die Äußerungen zu § 31 des Entwurfs.

Zu § 49 des Entwurfs (Befreiung von Gebühren, Abgaben 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 infolge der vorgeschlagenen Registrierungsfreiheit für Standardverarbeitungen sich die Einnahmen aus dieser Gebühr zusätzlich verringern werden, sodaß ihr Entfall noch weniger budgetrelevant ist.

Zu den §§ 50 und 51 des Entwurfs (Informationsaustausch mit den anderen EU-Mitgliedsstaaten und der Europäischen Kommission):

Die Bestimmungen der §§ 50 und 51 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.

Zu § 52 des Entwurfs (Inkrafttreten):

Die Richtlinie 95/46/EG sieht eine Frist von drei Jahren ab Inkrafttreten (24. Oktober 1995) für die Umsetzung in die nationalen Rechtsordnungen vor. Dementsprechend sollte das DSG 1998 spätestens mit 24. Oktober 1998 in Kraft treten.

Zu § 53 des Entwurfs (Übergangsbestimmungen):

Gemäß Art. 32 Abs. 2 der Richtlinie haben Auftraggeber von Datenverarbeitungen, die zum Zeitpunkt des Inkrafttretens der innerstaatlichen Vorschriften, die in Umsetzung der Richtlinie erlassen wurden, bereits operational sind, dafür zu sorgen, daß diese Verarbeitungen binnen drei Jahren mit den neuen innerstaatlichen Vorschriften in Einklang gebracht werden. Diesem Auftrag dienen die Absätze 1 und 2, in welchen für jene Fälle, in denen geänderte Zulässigkeitsvoraussetzungen nach der neuen Rechtslage vorliegen könnten, eine neuerliche Registrierung bzw. Genehmigung einzuholen sein wird. Die Frist hiefür liegt innerhalb des Dreijahres-Zeitraums und ist einfachheitshalber mit dem 1.1.2001 festgesetzt.