



REPUBLIK ÖSTERREICH
BUNDESKANZLERAMT

Datenschutz
245/ME

A-1010 Wien, Ballhausplatz 1
Tel. (0222) 531 15/0
Fax: (0222) 531 15/2690
Fernschreib-Nr. 1370-900
DVR: 0000019

GZ 810.026/17-V/3/98

An
die Parlementsdirektion
den Rechnungshof
alle Bundesministerien
alle Sektionen des Bundeskanzleramtes
alle Ämter der Landesregierungen
die Verbindungsstelle der Bundesländer beim Amt der Niederösterreichischen
Landesregierung
den Österreichischen Städtebund
den Österreichischen Gemeindebund
die Wirtschaftskammer Österreichs
die Bundesarbeitskammer
die Österreichische Ärztekammer
den Hauptverband der österreichischen Sozialversicherungsträger
die Österreichische Bischofskonferenz
den evangelischen Oberkirchenrat A und HB Wien
das Völkerrechtsbüro
den Verband österreichischer Zeitungen

Gesetzesentwurf	
Zl. <i>Zy 40</i>	-GE/19 ⁹⁸
Datum <i>12. 9. 1998</i>	
Verteilt <i>11. 9. 98</i>	

Dr. Moser

Betrifft: Datenschutzgesetz 1998

In der Anlage wird eine aufgrund der Ergebnisse des Begutachtungsverfahrens erstellte Neufassung des Textes für ein Datenschutzgesetz 1998 übermittelt mit dem Ersuchen um allfällige Rückäußerung bis 21. September 1998

1. September 1998
Für den Bundeskanzler:
KOTSCHY

Für die Richtigkeit
der Ausfertigung:
Müller

Datenschutzgesetz 1998

Entwurf

**Bundesgesetz
über den Schutz personenbezogener Daten
(Datenschutzgesetz 1998 - DSGVO)**

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 daran ein schutzwürdiges Interesse hat.

(2) Soweit die Verwendung von Daten des Betroffenen nicht in seinem eigenen Interesse unerlässlich ist oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Rechtes nach Abs.1 durch die Verwendung personenbezogener Daten 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 zulässiger Beschränkungen darf nur die jeweils gelindeste zielführende Art des Eingriffs in das Grundrecht vorgesehen werden.

(3) Beschränkungen des Anspruchs auf Geheimhaltung durch Verwendung von Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben sind ausschließlich

1. in den in § 7a geregelten Fällen zulässig sowie
2. auf Grund von Gesetzen, die die Verwendung der genannten Datenarten zur Wahrung wichtiger öffentlicher Interessen vorsehen und gleichzeitig angemessene Garantien zur Wahrung der schutzwürdigen Geheimhaltungsinteressen der Betroffenen festlegen.

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

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

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

(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 gemäß Abs.4 Z 1 ist, soweit nicht Akte der Gesetzgebung oder der Gerichtsbarkeit betroffen sind, die Datenschutzkommission (§§ 30 ff) zuständig.**

RÄUMLICHER ANWENDUNGSBEREICH

§ 2. (1) Die Bestimmungen dieses Bundesgesetzes sind anzuwenden auf die Verwendung von personenbezogenen Daten im Inland (§ 3 Z 14). 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 eines Auftraggebers (§ 3 Z 4) erfolgt. Als Niederlassung gilt jede durch feste Einrichtungen an einem bestimmten Ort räumlich und funktional abgegrenzte Organisationseinheit mit oder ohne Rechtspersönlichkeit, die tatsächlich Tätigkeiten ausübt.

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

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

(4) Von den Absätzen 1 bis 3 abweichende gesetzliche Regelungen sind nur außerhalb des Bereichs der Zuständigkeiten der Europäischen Gemeinschaften zulässig.

Artikel 2

1. Abschnitt

ALLGEMEINES

DEFINITIONEN

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

1. „Daten“ („personenbezogene Daten“): Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist. Nur „indirekt personenbezogen“ sind Daten für einen Auftraggeber (Z 4) Dienstleister (Z 5) oder Übermittlungsempfänger (vgl. Z 10) dann, wenn der Personenbezug der Daten so gestaltet ist, daß dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann;
2. „sensible Daten“: Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinungen, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugungen, Gesundheit oder ihr Sexualleben;
3. „Betroffener“: Jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;
4. „Auftraggeber“: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise deren Geschäftsapparate, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hierzu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie Daten einem anderen zur Herstellung eines von ihnen aufgetragenen Werkes übergeben und der Auftragnehmer die Entscheidung trifft, die Daten zur Herstellung des Werkes zu verarbeiten, es sei denn, daß ihm dies anlässlich der Auftragserteilung ausdrücklich untersagt wurde.

5. „Dienstleister“: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft **beziehungsweise deren Geschäftsapparate, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes übergeben wurden, verwenden (Z 8), es sei denn, daß ihnen die Verarbeitung (Z 9) der Daten anlässlich der Auftragserteilung ausdrücklich untersagt wurde.**

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

7. „Datenanwendung“ („Applikation“): **die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (vgl. Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung); [als Datenanwendung gilt weiters auch jede nicht automationsunterstützt, sondern ausschließlich manuell geführte Datei (manuelle Datenanwendung)];**

8. „Verwenden von Daten“: **Jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 11) von Daten.**

9. „Verarbeiten von Daten“: **das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen von Daten zwischen Auftraggeber und Dienstleistern, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittels (Z 11) von Daten;**

10. „Ermitteln von Daten“: Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;
11. „Übermitteln von Daten“: die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet (Z 12) des Auftraggebers;
12. „Aufgabengebiet“: eines von mehreren Tätigkeitsfeldern eines Auftraggebers, das in seinem Umfang nach der Verkehrsauffassung oder der verwaltungsüblichen Zuständigkeitsverteilung geeignet ist, für sich allein den gesamten Geschäftsbereich eines Auftraggebers zu bilden;
13. „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;
14. Inland: jene Gebiete und Institutionen, für welche gemäß Verfassungs- oder Völkerrecht die österreichischen datenschutzrechtlichen Vorschriften gelten.

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

§ 5. (1) Daten dürfen nur

1. nach Treu und Glauben und auf rechtmäßige Weise verwendet werden;
2. für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden; die Weiterverwendung für wissenschaftliche und statistische Zwecke ist nach Maßgabe besonderer gesetzlicher Vorschriften zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, daß sie im Ergebnis sachlich richtig und, wenn angesichts des Verwendungszwecks nötig, auf den neuesten Stand gebracht sind; ist dies nicht möglich, ist die Richtigkeit und Vollständigkeit der aus den verwendeten Daten abzuleitenden Information durch entsprechende Anmerkungen sicherzustellen, wenn dies im Hinblick auf die schutzwürdigen Betroffeneninteressen geboten ist;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

(2) Der Auftraggeber trägt bei seinen Datenanwendungen die Verantwortung für die Einhaltung der in Abs. 1 genannten Grundsätze; dies gilt - nach den näheren Bestimmungen des § 29 - auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

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

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

ZULÄSSIGKEIT DER VERARBEITUNG VON DATEN

§ 6. (1) In einer Datenanwendung dürfen Daten verarbeitet werden, wenn hierfür eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung besteht. Dies liegt nur dann vor, wenn die Verarbeitung von Daten für einen bestimmten Verarbeitungszweck unter Nennung der berechtigten Auftraggeber(kreise), der zulässigerweise verarbeiteten Datenarten und der Betroffenenkreise gesetzlich vorgesehen ist.

(2) Mangels einer solchen gesetzlichen Grundlage dürfen Daten - abgesehen von den Fällen des Abs.3 - nur dann verarbeitet werden, wenn die Datenanwendung

1. für die Verwirklichung eines berechtigten Zwecks des Auftraggebers erforderlich ist
- und
2. schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt (vgl. § 8).

(3) Die Zulässigkeit der Verarbeitung von Daten für die in Abschnitt 7 genannten besonderen Zwecke ergibt sich aus den Bestimmungen dieses Abschnitts.

(4) Werden Daten in einer der besonderen Verwendungsarten des Abschnittes 8 verarbeitet, gilt Absatz 2 nach Maßgabe der Bestimmungen des 8. Abschnitts.

(5) Bei jeder Verarbeitung von Daten ist § 5 Abs.1 zu befolgen.

ZULÄSSIGKEIT DER ÜBERMITTLUNG VON DATEN

§ 7. (1) Der Auftraggeber einer Datenanwendung darf Daten aus dieser Datenanwendung übermitteln, wenn hiezu eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung besteht. Dies liegt nur dann vor, wenn die Übermittlung von Daten zu einem bestimmten Zweck unter gleichzeitiger Nennung der ermächtigten oder verpflichteten Auftraggeber(kreise), der von der Übermittlung betroffenen Datenarten, der zugehörigen Betroffenenkreise und der Empfänger(kreise) gesetzlich vorgesehen ist.

(2) Mangels einer derartigen gesetzlichen Grundlage dürfen Daten - abgesehen von den Fällen der Abs.3 und 4 - nur dann übermittelt werden, wenn

1. die Übermittlung nicht gesetzlich verboten ist, wie etwa infolge gesetzlicher Verschwiegenheitspflichten und
2. die zu übermittelnden Daten aus einer iSd §§ 5 und 6 rechtlich zulässigen Datenanwendung stammen und
2. der Empfänger einen ausreichenden berechtigten Zweck für die Vornahme jener Tätigkeit besitzt, für die die Übermittlung erfolgt und
3. die Übermittlung zur Wahrung eines überwiegenden berechtigten Interesses erforderlich ist, sodaß die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt sind (vgl. § 7a).

(3) Die Zulässigkeit von Übermittlungen im Rahmen der im 8. Abschnitt geregelten besonderen Verwendungszwecke ergibt sich aus den Bestimmungen dieses Abschnitts.

(4) Liegt eine der besondern Verwendungsarten des 9. Abschnitts vor, richtet sich die Zulässigkeit von Übermittlungen in diesen Fällen nach den Bestimmungen dieses Abschnitts.

(5) Bei jeder Übermittlung von Daten ist § 5 Abs.1 zu befolgen.

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

SCHUTZWÜRDIGE GEHEIMHALTUNGSINTERESSEN

§ 7a. (1) Bei Verwendung nicht-sensibler Daten sind - abgesehen von den Fällen des Absatz 3 - schutzwürdige Geheimhaltungsinteressen des Betroffenen im Sinne der §§ 6 Abs.2 Z 2 und 7 Abs.2 Z 3 insbesondere dann nicht verletzt, wenn

- 1. zulässigerweise veröffentlichte Daten verarbeitet oder übermittelt werden;**
- 2. Daten zur Erfüllung gesetzlicher Vorschriften, auch wenn diese nicht den Charakter von Regelungen nach § 6 Abs.1 oder § 7 Abs.1 haben, verwendet werden,**
- 3. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt;**
- 4. die Verwendung zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenenem notwendig und der Betroffenen hierüber entsprechend informiert ist;**
- 5. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor einer Behörde erforderlich ist und die Daten rechtmäßig ermittelt wurden;**
- 6. die Verarbeitung oder Übermittlung zur Wahrung wichtiger Interessen des Betroffenen erforderlich ist und eine der Z 3 entsprechende Zustimmung nicht rechtzeitig eingeholt werden konnte;**
- 7. die Verwendung zur Wahrung lebenswichtiger Interessen eines anderen Menschen notwendig ist;**
- 8. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben.**

(2) (Verfassungsbestimmung) Bei der Verwendung sensibler Daten werden schutzwürdige Geheimhaltungsinteressen der Betroffenen nur in folgenden Fällen nicht verletzt:

- 1. in den Fällen des Absatz 1 Z 2, 5, 7 und 8;**
- 2. wenn Daten verwendet werden, die der Betroffene offenbar selbst an die Öffentlichkeit gebracht hat;**
- 3. wenn die ausdrückliche Zustimmung des Betroffenen vorliegt ;**
- 4 wenn die Verwendung zur Wahrung lebenswichtiger Interessen des Betroffenen erforderlich ist und seine Zustimmung nicht rechtzeitig eingeholt werden konnte;**
- 5. wenn die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- und Dienstrechts Rechnung zu tragen; dies gilt insbesondere auch für die Wahrnehmung der Aufgaben des Betriebsrates gemäß dem Arbeitsverfassungsgesetz;**
- 6. wenn die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen;**
- 7. wenn nicht auf Gewinn gerichtete Vereinigungen mit politischem oder weltanschaulichem Tätigkeitszweck 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, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.**

(3) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn solche Daten durch Auftraggeber des öffentlichen Bereichs für die in § 15 Abs.5 genannten Zwecke verwendet werden oder wenn sich sonst die Zulässigkeit der Verwendung aus gesetzlichen Vorschriften ergibt.

BESONDERE BESTIMMUNGEN FÜR DEN ÖFFENTLICHEN BEREICH

§ 7b. (1) Bei einem Auftraggeber des öffentlichen Bereichs, der in Vollziehung der Gesetze tätig wird, ist eine Datenanwendung dann für die Verwirklichung seines berechtigten Zwecks (§ 6 Abs. 2 Z 1) erforderlich, wenn die Benützung der in der Datenanwendung enthaltenen Daten für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe eine wesentliche Voraussetzung bildet.

(2) Wenn eine Übermittlungen aus Datenanwendungen, die von Auftraggebern des öffentlichen Bereichs in Vollziehung der Gesetze vorgenommen werden, in Erfüllung des Rechtes beziehungsweise der Verpflichtung zur Amtshilfe geschieht, sind überwiegende schutzwürdige Geheimhaltungsinteressen eines Betroffenen nicht verletzt.

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, soweit ihm dies zumutbar ist, 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 auch dann ohne Genehmigung im Sinne des § 11 zulässig, wenn davon Daten juristischer Personen betroffen sind.

(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 ins Ausland (vgl. § 2 Abs. 1) dann genehmigungsfrei, wenn

1. die Übermittlung (Überlassung) ins Ausland aufgrund von Rechtsvorschriften geschieht, 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
/ 2a. Zustimmung durch Betriebsvereinbarung/
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. Daten aus Datenanwendungen gemäß §§ 41 oder 44 oder Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt (überlassen) werden oder
5. 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 ins Ausland erfüllt werden kann oder
6. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und dem Auftraggeber rechtmäßig zugekommene Daten betrifft, oder
7. es sich um Übermittlungen oder Überlassungen handelt, die in einer Standardanwendung (§ 15 Abs. 4 Z 5) /oder Musterverordnung (§16 Abs. 2)/ 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 Menschen so dringlich ist, daß eine Genehmigung der Datenschutzkommission gemäß § 11 nicht eingeholt werden kann, ohne die genannten Interessen 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 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 insbesondere 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 Datenanwendung 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 Datenanwendungen die dem Dienstleister genehmigte Überlassung erfolgen soll; dies ist im Register anzumerken.

3. Abschnitt

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 im notwendigen Ausmaß nachvollzogen werden können,**
8. **eine Dokumentation über die nach Z. 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.**

(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) Arbeitnehmer (Dienstnehmer) eines Auftraggebers oder Dienstleisters dürfen Daten aus Datenanwendungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten nur auf Grund einer ausdrücklichen Anordnung der anordnungsbefugten Organe des Auftraggebers oder Dienstleisters übermitteln (Datengeheimnis).

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

(3) Die anordnungsbefugten Organe eines Auftraggebers oder Dienstleisters dürfen eine Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies nach den Bestimmungen dieses Bundesgesetzes zulässig ist. Sie haben die von der Anordnung betroffenen Arbeitnehmer (Dienstnehmer) über die für sie geltenden Übermittlungsanordnungen und über die strafrechtlichen Folgen einer Verletzung des Datengeheimnisses zu belehren.

(4) Aus der Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen die §§ 5, 7 oder 11 darf einem Arbeitnehmer (Dienstnehmer) kein Nachteil erwachsen.

4. 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) Datenanwendungen, die nicht unter § 16 Abs. 2 fallen und die

1. sensible Daten enthalten oder
2. die Auskunft über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder
3. strafrechtlich relevante Sachverhalte betreffen oder
4. in Form eines Informationsverbundsystems (§ 46) durchgeführt werden sollen, dürfen erst nach ihrer Prüfung und Registrierung durch die Datenschutzkommission aufgenommen werden (Vorabkontrolle) oder sobald die Datenschutzkommission gemäß § 17 Abs.2 die Erlaubnis zur Aufnahme der Verarbeitung erteilt hat.

(3) Die Vorabkontrolle gilt nicht für Datenanwendungen, die innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betreffen.

(4) Nicht meldepflichtig sind Datenanwendungen, die

1. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§41);
2. gemäß §§ 45 und 45a vorgenommen werden;
3. ausschließlich veröffentlichte Daten enthalten, deren Veröffentlichung nicht offenbar unzulässig ist;
4. die Führung von Registern oder Verzeichnissen betreffen, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses;
5. Standardanwendung darstellen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der zu verwendenden Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

(5) Datenanwendungen für Zwecke

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich,
 2. der Sicherung der Einsatzbereitschaft des Bundesheers oder der umfassenden Landesverteidigung,
 3. des Schutzes wichtiger wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der europäischen Union oder
 4. der Strafrechtspflege
- sind, soweit dies zur Verwirklichung des Zweckes der Datenverarbeitung unerlässlich ist, von der Meldepflicht nach Abs.1 ausgenommen.

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 der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben;**
- 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 notwendig ist - 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 gleichartige Datenanwendungen vorzunehmen haben und die Voraussetzungen für die Erklärung zur Standardanwendung nicht vorliegen, kann der Bundeskanzler durch Verordnung eine Mustermeldung festlegen. Meldungen über Datenanwendungen, 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 Datenanwendung 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 Datenanwendung 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) Die Datenschutzkommission hat alle Meldungen zu prüfen. Kommt sie hiebei zur Auffassung, daß eine Meldung im Sinne des § 16 Abs. 3 mangelhaft ist, so ist dem Auftraggeber längstens innerhalb von zwei Monaten nach Einlangen der Meldung die Verbesserung des Mangels unter Setzung einer Frist aufzutragen. Wird innerhalb von zwei Monaten nach Erstattung der Meldung weder ein Registerauszug zugesandt noch ein Auftrag zur Verbesserung erteilt, gilt die Meldepflicht dennoch als erfüllt.

(2) Bei Verarbeitungen, die gemäß § 15 Abs.2 der Vorabkontrolle unterliegen, ist gleichzeitig mit dem Auftrag zur Verbesserung darüber abzusprechen, ob die Verarbeitung bereits aufgenommen werden darf oder ob dies wegen Mangelhaftigkeit hinsichtlich der Rechtsgrundlagen der gemeldeten Datenanwendung nicht zulässig ist. Ergeht innerhalb von zwei Monaten nach Erstattung der Meldung kein Auftrag zur Verbesserung, darf die Verarbeitung jedenfalls aufgenommen werden.

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

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

(2) Dem Auftraggeber ist die Durchführung der Registrierung schriftlich in Form eines Registerauszuges mitzuteilen. Der Auszug hat bei der erstmaligen Meldung eines Auftraggebers auch die ihm endgültig zugeteilte Registernummer anzuführen.

RICHTIGSTELLUNG DES REGISTERS

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

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

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

(4) Werden der Datenschutzkommission andere als die in Abs. 2 bezeichneten Umstände bekannt, die den Verdacht der Mangelhaftigkeit einer Registrierung iSd § 16 Abs. 3 oder der rechtswidrigen Unterlassung einer Meldung begründen, so hat die Datenschutzkommission ein Verfahren zur Feststellung des für die Erfüllung der Meldepflicht erheblichen Sachverhalts einzuleiten und das Datenverarbeitungsregister entsprechend dem Ergebnis des Verfahrens zu berichtigen.

**PFLICHT ZUR OFFENLEGUNG
NICHT MELDEPFLICHTIGER DATENANWENDUNGEN**

§ 20. Soweit es sich nicht um die Verarbeitung von Daten für private Zwecke gemäß § 41 oder für publizistische Zwecke gemäß § 44 oder für die in § 15 Abs.5 genannten Zwecke handelt, hat jeder Auftraggeber von nicht-meldepflichtigen Datenanwendungen ein Verzeichnis zu führen, aus welchem die Zweckbestimmung der Anwendungen und - soweit sich dies nicht bereits aus Verordnungen gemäß §§ 15 oder 16 ergibt - die verarbeiteten Datenarten, Betroffenenkreise und Empfängerkreise im In- und Ausland hervorgehen.

(2) In dieses Verzeichnis ist jedermann auf Antrag Einsicht zu gewähren, sofern nicht offensichtlich ist, daß die Einsicht nicht zur Wahrung von Rechten nach diesem Bundesgesetz dient.

(3) Nicht-meldepflichtige Datenanwendungen, die auch nicht in das Verzeichnis gemäß Abs.1 aufzunehmen sind, sind der Datenschutzkommission bei Ausübung ihrer Kontrollaufgaben gemäß § 26 offenzulegen.

INFORMATIONSPFLICHT DES AUFTRAGGEBERS

§ 21. (1) Der Auftraggeber einer Datenanwendung hat vor Aufnahme der Verarbeitung von Daten die Betroffenen in geeigneter Weise zu informieren über

1. den Zweck der Datenanwendung, für die die Daten erhoben werden, und über
2. Namen und Adresse des Auftraggebers

sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.

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

1. die Datenverwendung durch Gesetz oder Verordnung ausdrücklich vorgesehen ist oder
2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder
3. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik in den Fällen des § 42 Abs.1 ermittelt werden.

(3) Die Informationspflicht entfällt für jene nicht-meldepflichtigen Datenanwendungen, die in der gemäß § 20 Abs.1 zu führende Liste nicht angeführt werden müssen.

(4) Über Absatz 1 hinausgehende Informationen sind im notwendigen Umfang und in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist, insbesondere wenn

1. gegen eine bestimmte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 25 Abs.2 besteht; könnte, ob
2. es nach den Umständen des Falles für den Betroffenen nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen verpflichtet ist;
3. Daten in einem Informationsverbundsystem verarbeitet werden sollen.

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 hierbei um eine meldepflichtige Datenverarbeitung, ist die Registernummer des Auftraggebers beizufügen.

5. 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 die verarbeiteten Daten, ihre Herkunft, allfällige Empfänger, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form 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 berechnigte 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, des Schutzes wichtiger wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union sowie der Strafrechtspflege ergeben.

(3) Keinem Recht auf Auskunft unterliegen Datenanwendungen, die zulässigerweise zur öffentlichen Einsicht bestimmt sind.

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

(5) Eine Auskunft ist unentgeltlich zu erteilen, wenn sie Datenanwendungen 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.

(6) Innerhalb von 8 Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird.

Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Betroffene am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(7) 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 verarbeitete Daten unverzüglich richtigzustellen oder zu löschen, und zwar

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

Die Unrichtigkeit oder Unvollständigkeit verwendeter Daten bewirkt nur dann eine Pflicht zur Richtigstellung, wenn die Unrichtigkeit Daten betrifft, die für den Zweck der Datenanwendung Bedeutung haben beziehungsweise 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 8 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 schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergibt, Widerspruch zu erheben, sofern die Verwendung nicht gesetzlich angeordnet ist. Der Auftraggeber der Datenanwendung hat den Betroffenen bei Vorliegen der besonderen Voraussetzungen binnen 8 Wochen aus seiner Datenverarbeitung zu löschen beziehungsweise eine beeinspruchte Übermittlung zu unterlassen.

(2) Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datei kann der Betroffene jederzeit auch ohne Nachweis der Verletzung seiner schutzwürdigen Geheimhaltungsinteressen Widerspruch mit dem Anspruch auf Löschung erheben.

6. Abschnitt

RECHTSSCHUTZ

KONTROLLBEFUGNISSE DER DATENSCHUTZKOMMISSION

§ 26. (1) Jedermann kann sich 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, mit einer Eingabe an die Datenschutzkommission wenden. Der Einschreiter ist darüber zu informieren, wie mit seiner Eingabe verfahren wurde.

(2) Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechtsvorschriften Einschau in Datenanwendungen und die diesbezüglichen Unterlagen begehren und Aufklärung vom Auftraggeber der überprüften Datenanwendung verlangen. Zu diesem Zweck sind die Datenschutzkommission und die von ihr bestellten Kontrollorgane berechtigt, nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) Räume, in welchen Datenanwendungen vorgenommen werden, zu betreten, Datenverarbeitungsanlagen in Betrieb zu setzen, die zu überprüfenden Verarbeitungen durchzuführen, Testprogramme zur Prüfung des Verarbeitungsablaufs einzusetzen sowie Kopien von Datenträgern herzustellen.

(3) Der Auftraggeber (Dienstleister) hat die für die Einschau notwendige Hilfestellung zu leisten. Die Kontrolltätigkeit ist unter möglicher Schonung der Rechte des Auftraggebers (Dienstleisters) und Dritter auszuüben. Informationen, die der Datenschutzkommission oder ihren Beauftragten im Rahmen der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden.

(4) Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzkommission Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzkommission je nach der Art des Verstoßes gegen Vorschriften dieses Bundesgesetzes von Amts wegen insbesondere

1. ein Verfahren zur Überprüfung der Registrierung gemäß § 19 Abs. 4 einleiten, oder
2. Anzeige zur Einleitung eines Strafverfahrens gemäß §§ 47 und 48 erstatten, 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, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, daß der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung kann von der Datenschutzkommission der Öffentlichkeit in geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtsverschwiegenheit entgegensteht.

(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 hat den Unabhängigen Datenschutzkontrollstellen der anderen Mitgliedstaaten der Europäischen Union über Ersuchen zu leisten..

BESCHWERDE AN DIE DATENSCHUTZKOMMISSION

§ 27. (1) Die Datenschutzkommission erkennt auf Antrag des Betroffenen über behauptete Verletzungen des Auskunftsrechts (§ 23), soweit sich das Auskunftsbegehren nicht auf Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(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, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist.

(3) Bei Gefahr im Verzug für den Beschwerdeführer kann die Datenschutzkommission im Falle des Abs.2 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.**

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) Zur Sicherung der auf dieses Bundesgesetz gestützten Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden, auch wenn die in § 381 EO bezeichneten Voraussetzungen nicht zutreffen.

(4) Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung nach diesem Bundesgesetz ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat. Klagen des Betroffenen können aber auch bei dem Landesgericht erhoben werden, in dessen Sprengel der Auftraggeber oder der Dienstleister seinen gewöhnlichen Aufenthalt oder Sitz hat.

(5) Die Datenschutzkommission 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.

(6) 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) Ein Auftraggeber oder Dienstleister, der Daten schuldhaft entgegen den Bestimmungen dieses Bundesgesetzes verwendet, hat dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen. In besonders schwerwiegenden Fällen, insbesondere bei der Verwendung der in § 15 Abs. 2 Z 1 bis 3 genannten Daten, hat der Betroffene zusätzlich Anspruch auf eine angemessene Entschädigung für die erlittene Beeinträchtigung, deren Höhe S 260. 000,-- nicht übersteigt.

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

(3) Der Auftraggeber sowie der Dienstleister können sich von ihrer Haftung befreien, wenn sie nachweisen daß der Umstand, durch den der Schaden eingetreten ist, ihm oder seinen Leuten (Abs. 2) nicht zur Last gelegt werden kann. / § 11 PHG betreffend Mitschuld des Betroffenen oder Dritter/.

(4) Die Zuständigkeit für Klagen nach Abs. 1 richtet sich nach § 28 Abs. 4.

7. 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, sofern das Auskunftsbegehren nicht Akte der Gesetzgebung oder der Gerichtsbarkeit betrifft;**
- 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 Gesetzgebung oder der Gerichtsbarkeit 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 aus (§ 26) und erstattet hiebei Empfehlungen an Auftraggeber von Datenverarbeitungen. Die Datenschutzkommission übt die 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 wesentliche Fragen des Datenschutzes unmittelbar betreffen.

(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 Dreivorschlag 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 Mitglieds an dessen Stelle. **Die Funktionsperiode des Ersatzmitglieds endet mit der Funktionsperiode des Mitglieds; für den Fall der vorzeitigen Beendigung der Funktionsperiode des Mitglieds gilt Absatz 8.**

(5) Der Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;
2. Personen, die zum Nationalrat nicht wählbar sind.

(6) Hat ein Mitglied der Datenschutzkommission Einladungen zu drei aufeinanderfolgenden Sitzungen ohne genügende Entschuldigung keine Folge geleistet oder tritt bei einem Mitglied ein Ausschließungsgrund des Abs. 5 nachträglich ein, so hat dies nach seiner Anhörung die Datenschutzkommission festzustellen. Diese Feststellung hat den Verlust der Mitgliedschaft zur Folge. Im übrigen kann ein Mitglied der Datenschutzkommission nur aus einem schwerwiegenden Grund durch Beschluß der Datenschutzkommission, dem mindestens 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 Ersatzmitglied zu bestellen. **Scheidet ein Ersatzmitglied vorzeitig aus, ist umgehend eines neues Ersatzmitglied zu bestellen.**

(9) Die Mitglieder und Ersatzmitglieder der Datenschutzkommission haben Anspruch auf Ersatz der Reisekosten (Gebührenstufe 3) nach Maßgabe der für Bundesbeamte geltenden Rechtsvorschriften. Sie haben ferner Anspruch auf eine dem Zeit- und Arbeitsaufwand entsprechende Vergütung, die auf Antrag des Bundeskanzlers von der Bundesregierung durch Verordnung festzusetzen ist.

WEISUNGSFREIHEIT DER DATENSCHUTZKOMMISSION

§ 33. (Verfassungsbestimmung)

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

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

ORGANISATION UND GESCHÄFTSFÜHRUNG DER DATENSCHUTZKOMMISSION

§ 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.

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. Eine Vorstellung gegen einen gemäß § 19 Abs. 3 ergangenen Bescheid hat aufschiebende Wirkung.

(2) Im Registrierungsverfahren gemäß § 15 ff und im Genehmigungsverfahren gemäß § 10 f haben Auftraggeber des öffentlichen Bereichs auch hinsichtlich der Datenanwendungen, die sie in Vollziehung der Gesetze durchführen, Parteistellung.

(3) Gegen andere als die in Abs. 1 genannten 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. Die Beschwerde an den Verwaltungsgerichtshof hat 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 datenschutzrechtlicher 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.**

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

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 3) nach Maßgabe der für Bundesbeamte 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 hierfür das notwendige Personal zur Verfügung zu stellen. Bei ihrer Tätigkeit für den Datenschutzrat sind die Bediensteten des Bundeskanzleramtes fachlich an die Weisungen des Vorsitzenden des Datenschutzrates gebunden.

SITZUNGEN UND BESCHLUßFASSUNG DES DATENSCHUTZRATES

§ 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 Stimmgleichheit 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.

8. Abschnitt

BESONDERE VERWENDUNGSZWECKE VON DATEN

PRIVATE ZWECKE

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

(2) Daten, die eine natürliche Personen für ausschließlich persönliche oder familiäre Tätigkeiten verarbeitet, dürfen für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.

WISSENSCHAFTLICHE FORSCHUNG UND STATISTIK

§ 42. (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, dürfen vom Auftraggeber der Untersuchung alle Daten herangezogen werden, die

1. öffentlich zugänglich sind oder
2. der Auftraggeber für andere Untersuchungen oder auch andere Zwecke zulässigerweise ermittelt hat oder
3. für den Auftraggeber nur indirekt personenbezogen sind.

(2) Liegt kein Fall des Abs. 1 Z 1 bis 3 vor, dürfen nur solche Daten für die in Absatz 1 genannten Zwecke verwendet werden, die

1. gemäß besonderen gesetzlichen Vorschriften oder
2. mit Zustimmung des Betroffenen oder
3. mit Genehmigung der Datenschutzkommission gemäß Abs.4

ermittelt wurden.

(3) Die Ermittlung von Daten für wissenschaftliche Untersuchungen mit personenbezogenen Ergebnissen ist nur unter den in Absatz 2 genannten Voraussetzungen zulässig.

(4) Soweit eine Genehmigung der Datenschutzkommission zur Verwendung von personenbezogenen Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß Abs. 1 oder 3 notwendig ist, ist sie zu erteilen, wenn die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und wenn überdies ein die schutzwürdigen Geheimhaltungsinteressen der Betroffenen überwiegendes öffentliches Interesse an der Durchführung der wissenschaftlichen (statistischen) Untersuchung glaubhaft gemacht wird. Sollen sensible Daten übermittelt werden, muß ein wichtiges öffentliches Interesse an der wissenschaftlichen Untersuchung glaubhaft gemacht werden und es muß sichergestellt sein, daß die Daten beim Empfänger nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder die ihre datenschutzrechtliche Verlässlichkeit sonst glaubhaft gemacht haben. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung von sensiblen Daten, notwendig ist.

(5) Rechtliche Beschränkungen für die Zulässigkeit der Benützung von Daten, die aus anderen als datenschutzrechtlichen, insbesondere urheberrechtlichen Gründen bestehen, bleiben unberührt.

(6) Auch in jenen Fällen, in welchen die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß Abs. 1 bis 3 in personenbezogener Form zulässig ist, sind die Daten in nur indirekt personenbezogener Form zu verwenden, wenn dies in einzelnen Abschnitten der Untersuchung möglich ist. Der Personenbezug der Daten ist unverzüglich gänzlich zu beseitigen, sobald er für die Untersuchung nicht mehr notwendig ist.

ZURVERFÜGUNGSTELLUNG VON ADRESSEN ZUR BENACHRICHTIGUNG UND BEFRAGUNG VON BETROFFENEN

§ 43. (1) Soweit gesetzlich nicht ausdrücklich anderes vorgesehen ist, bedarf die Übermittlung von Adreßdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung der Zustimmung der Betroffenen. Wenn allerdings angesichts des Auswahlkriteriums für den Betroffenenkreis und des Gegenstands der Benachrichtigung oder Befragung die Beeinträchtigung von Betroffenenrechten unwahrscheinlich ist,

1. bedarf es keiner Zustimmung, wenn Daten desselben Auftraggebers verwendet werden;
2. gilt als Zustimmung zur Übermittlung an Dritte auch die Nichterhebung eines Widerspruchs innerhalb offener Frist; Voraussetzung hierfür ist eine entsprechende Information des Betroffenen gemäß § 21;

(2) Soll die Übermittlung an Dritte

1. zum Zweck der Benachrichtigung oder Befragung aus einem wichtigen Interesse des Betroffenen selbst oder
2. aus einem öffentlichen Benachrichtigungs- oder Befragungsinteresse oder
3. zum Zweck der Befragung der Betroffenen für wissenschaftliche oder statistische Zwecke

erfolgen und würde die Einholung der Zustimmung der Betroffenen gemäß Abs.1 einen unverhältnismäßigen Aufwand erfordern, ist eine Übermittlung mit Genehmigung der Datenschutzkommission zulässig. Die Genehmigung ist zu erteilen, 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 glaubhaft gemacht werden, daß an der Übermittlung ein wichtiges öffentliches Interesse besteht. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.

(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 auch die zum Zweck der Auswahl der zu übermittelnden Daten notwendige Verarbeitung von Adreßdaten erfolgen.

PUBLIZISTISCHE TÄTIGKEIT

§ 44. (1) Soweit Medienunternehmen, Mediendienste oder ihre Mitarbeiter 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 5, 8, 9, 12 und 13 Anwendung.

(2) Die Verwendung von Daten für Tätigkeiten nach Abs. 1 ist insoweit zulässig, als dies zur Erfüllung der Informationsaufgabe der Medienunternehmer, Mediendienste und ihre Mitarbeiter 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.

9. Abschnitt

BESONDERE VERWENDUNGSARTEN VON DATEN

AUTOMATISIERTE EINZELENTSCHEIDUNGEN

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

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

1. dies gesetzlich ausdrücklich vorgesehen ist oder

2. die Entscheidung in Erfüllung eines Vertrages ergeht und dem Ersuchen der betreffenden Person auf Abschluß oder Erfüllung des Vertrages stattgegeben wurde oder die Wahrung ihrer berechtigten Interessen durch geeignete Maßnahmen - beispielsweise die Möglichkeit, ihren Standpunkt geltend zu machen - garantiert wird.

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

INDIREKT PERSONENBEZOGENE DATEN

§ 45a. (1) Soweit Daten ausschließlich in nur indirekt personenbezogener Form verwendet werden, findet

1. Abschnitt 2 nur mit der Maßgabe Anwendung, daß keine Verpflichtung zur Einholung einer Genehmigung nach § 11 und keine Verpflichtung zur Meldung nach § 15 besteht,
2. Abschnitt 5 keine Anwendung.

(2) Bei der Übermittlung von nur indirekt personenbezogenen Daten entfällt die Pflicht zur Einholung einer Genehmigung gemäß Abs.1 nur dann, wenn sichergestellt ist, daß der Empfänger den vollen Personenbezug mit rechtlich zulässigen Mitteln nicht wieder herstellen kann.

TEXTVERARBEITUNG

§ 45a. Die automationsunterstützte Erstellung und Archivierung von nicht strukturierten Texten (Textverarbeitung) gilt, soweit sie in unmittelbarem Zusammenhang mit einer Datei steht, als von der Meldung der Datenanwendung, in der die Datei verarbeitet wird, mitumfaßt.

INFORMATIONSVORBUNDSSYSTEME

§ 46. (1) Die gemeinsame Verwendung von Daten in einer Datenanwendung durch mehrere Auftraggeber in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von anderen dem System zur Verfügung gestellt wurden (Informationsverbundsystem), darf nur aufgrund einer ausdrücklichen gesetzlichen Ermächtigung für die im System stattfindenden Übermittlungen vorgenommen werden, wenn Daten iSd § 15 Abs. 2 Z 1 bis 3 verwendet werden.

(2) Bei jedem Informationsverbundsystem haben die Auftraggeber einen geeigneten Betreiber für das System zu bestellen und in der Meldung gemäß § 15 zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet der Betroffenenrechte gemäß § 23 hat der Betreiber jedem Betroffenen auf Antrag alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber zu finden; dasselbe gilt für diesbezügliche Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§12) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber nach dem Bestimmungen des § 29 Abs.3 befreien. Wird ein Informationsverbundsystem geführt, ohne daß eine entsprechende Meldung an die Datenschutzkommission unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.

(3) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten auf den Betreiber übertragen werden; soweit dies nicht durch Gesetz geschehen ist, ist dieser Pflichtenübergang gegenüber den Betroffenen und den für die Vollziehung dieses Gesetzes zuständigen Behörden nur wirksam, wenn er - aufgrund einer entsprechenden Meldung an die Datenschutzkommission - aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.

(4) Die Bestimmungen der Absätze 2 und 3 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 mit Daten, die er sich aus einer Datenanwendung verschafft hat, einem anderen widerrechtlich und vorsätzlich Schaden zufügt, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

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

Alternative 1:

§ 47. (1) Wer durch die rechtswidrige Benützung von Daten aus einer Datenanwendung einem anderen vorsätzlich Schaden zufügt, ist, wenn

Alternative 2:

§ 47. (1) Wer sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft,.....

VERWALTUNGSSTRAFBESTIMMUNG

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

- 1. sich vorsätzlich widerrechtlichen Zugang zu Datenanwendungen verschafft;**
- 2. eine widerrechtliche Anordnung im Sinne des § 13 Abs. 3 zu einer Übermittlung von Daten erteilt, die geeignet ist, die schutzwürdigen Geheimhaltungsinteressen eines Betroffenen zu verletzen;**
- 3. Daten in Verletzung des Datengeheimnisses (§ 13 Abs. 1) übermittelt und dabei schutzwürdige Geheimhaltungsinteressen von Betroffenen verletzt;**
- 4. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht;**
- 5. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 15 erfüllt zu haben;**
- 6. Daten ins Ausland übermittelt oder überläßt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 11 eingeholt zu haben;**
- 7. die gemäß § 12 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht läßt,**
- 8. seine Offenlegungs- oder Informationspflichten gemäß den §§ 20, 21 oder 22 verletzt;**
- 9. seiner Verpflichtung zur Beantwortung eines Auskunftsbegehrens gemäß § 23 Abs. 5 nicht entspricht;**
- 10. Daten vorsätzlich entgegen § 23 Abs. 6 löscht;**
- 11. Daten, die ihm gemäß §§ 42 oder 43 anvertraut wurden, vorsätzlich für andere Zwecke verwendet.**

(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, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat.**

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 BGBIG, 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 / Variante: 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 zugrunde zu legen.

(4) (Verfassungsbestimmung) Datenanwendungen, die für die in § 15 Abs. 5 genannten Zwecke unbedingt erforderlich sind, dürfen auch bei Fehlen einer im Sinne des § 1 Abs. 2 und 3 ausreichenden gesetzlichen Grundlage bis 31. 12. 2005 vorgenommen werden.

(5) Datenverwendungen, die gemäß § 46 Abs. 1 einer ausdrücklichen gesetzlichen Ermächtigung bedürfen, dürfen auch bei Fehlen einer solchen gesetzlichen Grundlage bis zum fortgeführt werden.

(6) Die Gesetze bleiben unbeschadet des Inkrafttretens dieses Bundesgesetzes in Geltung.

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.