

# Federal Act concerning the Protection of Personal Data (Datenschutzgesetz 2000 - DSG 2000)

The official German title is

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

The German Title "Datenschutzgesetz 2000" and the abbreviation "DSG 2000" should be used in English texts to avoid confusion.

Original promulgation:

Federal Law Gazette [*Bundesgesetzblatt*, short BGBl] part I No. 165/1999, on 17. August 1999

Amendments: Federal Law Gazette I No. 136/2001

BGBl. I Nr. 165/1999 (NR: GP XX RV 1613 AB 2028 S. 179.  
BR: 5992 AB 6034 S. 657.)  
[CELEX-Nr.: 395L0046]

BGBl. I Nr. 136/2001 (NR: GP XXI RV 742 AB 824 S. 81.  
BR: 6458 AB 6459 S. 681.)

Please note that all Austrian federal and state laws are available for free over the internet (in German) from <http://www.ris.bka.gv.at>

### Disclaimer:

This translation is unofficial. It has been made with great care, but linguistic compromises were unavoidable. The reader should also bear in mind that some provisions of the DSG 2000 will remain unclear without a certain background knowledge of the Austrian legal and political system. Please note that this law may be amended in the future, and check occasionally for updates.

## Inhaltsverzeichnis - Table of Contents

### Artikel 1 (Verfassungsbestimmung)

#### Article 1 (Constitutional Provision)

- § 1 Grundrecht auf Datenschutz  
Fundamental Right to Data Protection
- § 2 Zuständigkeit  
Legislative Power and Enforcement
- § 3 Räumlicher Anwendungsbereich  
Territorial Jurisdiction

### Artikel 2

#### Article 2

### 1. Abschnitt: Allgemeines

#### Part 1: General Provisions

- § 4 Definitionen  
Definitions
- § 5 Öffentlicher und privater Bereich  
Public and Private Sector

## **2. Abschnitt: Verwendung von Daten**

### **Part 2: Use of Data**

- § 6 Grundsätze  
Principles
- § 7 Zulässigkeit der Verwendung von Daten  
Legitimate Use of Data
- § 8 Schutzwürdige Geheimhaltungsinteressen bei Verwendung nichtsensibler Daten  
Interests in Secrecy Deserving Protection for the Use of Non-Sensitive Data
- § 9 Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten  
Interests in Secrecy Deserving Protection for the Use of Sensitive Data
- § 10 Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen  
Legitimate Committing of Data for Service Processing
- § 11 Pflichten des Dienstleisters - Obligations of the Processor
- § 12 Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland  
Transborder Transmission and Committing of Data not Subject to Licensing
- § 13 Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland  
Transborder Transmission and Committing of Data Subject to Licensing

## **3. Abschnitt: Datensicherheit**

### **Part 3 - Data Security**

- § 14 Datensicherheitsmaßnahmen  
Data Security Measures
- § 15 Datengeheimnis  
Confidentiality of Data

## **4. Abschnitt: Publizität der Datenverarbeitungen**

### **Part 4 - Publicity of Data Applications**

- § 16 Datenverarbeitungsregister  
Data Processing Register
- § 17 Meldepflicht des Auftraggebers  
Duty of the Controller to Notify
- § 18 Aufnahme der Verarbeitung  
Commencement of Processing
- § 19 Notwendiger Inhalt der Meldung  
Required Content of the Notification
- § 20 Prüfungs- und Verbesserungsverfahren  
Examination and Correction Procedure
- § 21 Registrierung  
Registration
- § 22 Richtigstellung des Registers  
Rectification of the Register
- § 23 Pflicht zur Offenlegung nichtmeldepflichtiger Datenanwendungen  
Obligation to Provide Information on Data Applications not Subject to Notification
- § 24 Informationspflicht des Auftraggebers  
The Controller's Duty to Provide Information
- § 25 Pflicht zur Offenlegung der Identität des Auftraggebers  
Obligation to Disclose the Identity of the Controller

## **5. Abschnitt: Die Rechte des Betroffenen**

### **Part 5 - Rights of the Data Subject**

- § 26 Auskunftsrecht  
Right to Information
- § 27 Recht auf Richtigstellung oder Löschung  
Right to Rectification and Erasure
- § 28 Widerspruchsrecht

- Right to Object  
§ 29 Die Rechte des Betroffenen bei Verwendung nur indirekt personenbezogener Daten  
Rights of the Data Subject concerning the Use of only Indirectly Personal Data

## **6. Abschnitt: Rechtsschutz**

### **Part 6 - Legal Remedies**

- § 30 Kontrollbefugnisse der Datenschutzkommission  
Duties of Supervision of the Data Protection Commission  
§ 31 Beschwerde an die Datenschutzkommission  
Complaint before the Data Protection Commission  
§ 32 Anrufung der Gerichte  
Court Action  
§ 33 Schadenersatz  
Damages  
§ 34 Gemeinsame Bestimmungen  
Common Provisions

## **7. Abschnitt: Kontrollorgane**

### **Part 7 - Control Bodies**

- § 35 Datenschutzkommission und Datenschutzrat  
Data Protection Commission and Data Protection Council  
§ 36 Zusammensetzung der Datenschutzkommission  
Composition of the Data Protection Commission  
§ 37 Weisungsfreiheit der Datenschutzkommission (Verfassungsbestimmung)  
Independence of the Data Protection Commission (Constitutional Provision)  
§ 38 Organisation und Geschäftsführung der Datenschutzkommission  
Organisation and Operation of the Data Protection Commission  
§ 39 Beschlüsse der Datenschutzkommission  
Decisions of the Data Protection Commission  
§ 40 Wirkung von Bescheiden der Datenschutzkommission und des geschäftsführenden Mitglieds  
Effects of Rulings of the Data Protection Commission and the Executive Member  
§ 41 Einrichtung und Aufgaben des Datenschutzrates  
Establishment and Duties of the Data Protection Council  
§ 42 Zusammensetzung des Datenschutzrates  
Composition of the Data Protection Council  
§ 43 Vorsitz und Geschäftsführung des Datenschutzrates  
Chairmanship and Operation of the Data Protection Council  
§ 44 Sitzungen und Beschlußfassung des Datenschutzrates  
Meetings and Decisions of the Data Protection Council

## **8. Abschnitt: Besondere Verwendungszwecke von Daten**

### **Part 8 - Special Purposes of Data Use**

- § 45 Private Zwecke  
Private Purposes  
§ 46 Wissenschaftliche Forschung und Statistik  
Scientific Research and Statistics  
§ 47 Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen  
Transmission of Addresses to Inform or Interview Data Subjects  
§ 48 Publizistische Tätigkeit  
Journalistic Purposes

## **9. Abschnitt: Besondere Verwendungsarten von Daten**

### **Part 9 - Special Uses of Data**

- § 49 Automatisierte Einzelentscheidungen  
Automated Individual Decisions  
§ 50 Informationsverbundsysteme

Joint Information Systems

**10. Abschnitt: Strafbestimmungen**

**Part 10 - Penal Provisions**

- § 51      Datenverwendung in Gewinn- oder Schädigungsabsicht  
            Use of Data with the Intention to make a Profit or to Cause Harm
- § 52      Verwaltungsstrafbestimmung  
            Administrative Penalties

**11. Abschnitt: Übergangs- und Schlussbestimmungen**

**Part 11 - Transitional and Final Provisions**

- § 53      Befreiung von Gebühren, Verwaltungsabgaben und vom Kostenersatz  
            Exemption from Fees
- § 54      Mitteilungen an die anderen Mitgliedstaaten der Europäischen Union und an die  
            Europäische Kommission  
            Communication to the European Commission and to the other Member States of the European Union
- § 55      Feststellungen der Europäischen Kommission  
            Measures of the European Commission
- § 56      Verwaltungsangelegenheiten gemäß Art. 30 B-VG  
            Administrative Matters pursuant to Art. 30 of the Federal Constitution
- § 57      Sprachliche Gleichbehandlung  
            Gender-Neutral Use of Language
- § 58      Manuelle Dateien  
            Manual Filing Systems
- § 59      Umsetzungshinweis  
            Implementation Notice
- § 60      Inkrafttreten  
            Entry into Force
- § 61      Übergangsbestimmungen  
            Transitional Provisions
- § 62      Verordnungserlassung  
            Enactment of Ordinances
- § 63      Verweisungen  
            References
- § 64      Vollziehung  
            Execution

## **Artikel 1**

### **(Verfassungsbestimmung)**

#### **Grundrecht auf Datenschutz**

**§ 1.** (1) Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

(2) Soweit die Verwendung von personenbezogenen Daten nicht im lebenswichtigen Interesse des Betroffenen oder mit seiner Zustimmung erfolgt, sind Beschränkungen des Anspruchs auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig, und zwar bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen, die aus den in Art. 8 Abs. 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), BGBl. Nr. 210/1958, genannten Gründen notwendig sind. Derartige Gesetze dürfen die Verwendung von Daten, die ihrer Art nach besonders schutzwürdig sind, nur zur Wahrung wichtiger öffentlicher Interessen vorsehen und müssen gleichzeitig angemessene Garantien für den Schutz der Geheimhaltungsinteressen der Betroffenen festlegen. Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.

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

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

(4) Beschränkungen der Rechte nach Abs. 3 sind nur unter den in Abs. 2 genannten Voraussetzungen zulässig.

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

## **Article 1**

### **(Constitutional Provision)**

#### **Fundamental Right to Data Protection**

**Sect. 1.** (1) Everybody shall have the right to secrecy for the personal data concerning him, especially with regard to his private and family life, insofar as he has an interest deserving such

protection. Such an interest is precluded when data cannot be subject to the right to secrecy due to their general availability or because they cannot be traced back to the data subject [*Betroffener*].

(2) Insofar personal data is not used in the vital interest of the data subject or with his consent, restrictions to the right to secrecy are only permitted to safeguard overriding legitimate interests of another, namely in case of an intervention by a public authority the restriction shall only be permitted based on laws<sup>1</sup> necessary for the reasons stated in Art. 8, para. 2 of the European Convention on Human Rights (Federal Law Gazette No. 210/1958). Such laws may provide for the use of data [*Verwendung von Daten*] that deserve special protection only in order to safeguard substantial public interests and shall provide suitable safeguards for the protection of the data subjects' interest in secrecy. Even in the case of permitted restrictions the intervention with the fundamental right shall be carried out using only the least intrusive of all effective methods.

(3) Everybody shall have, insofar as personal data concerning him are destined for automated processing or manual processing, i.e. in filing systems [*Dateien*] without automated processing, as provided for by law,

1. the right to obtain information as to who processes what data concerning him, where the data originated, for which purpose they are used, as well as to whom the data are transmitted;
2. the right to rectification of incorrect data and the right to erasure of illegally processed data.

(4) Restrictions of the rights according to para. 3 are only permitted under the conditions laid out in para. 2.

(5) The fundamental right to data protection, except the right to information [*Auskunftsrecht*], shall be asserted before the civil courts against organisations that are established according to private law, as long as they do not act in execution of laws. In all other cases the Data Protection Commission [*Datenschutzkommission*] shall be competent to render the decision, unless an act of Parliament or a judicial decision is concerned<sup>2</sup>.

## **Zuständigkeit**

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

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

## **Legislative Power and Enforcement**

**Sect. 2** (1) The Federation [*Bund*] shall have power to pass laws concerning the protection of personal data that are automatically processed.

(2) The Federation shall have power to execute such federal laws. Insofar as such data are used by a State [*Land*], on behalf of a State, by or on behalf of legal persons established by law within the powers of the States [*Länder*] these Federal Acts [*Bundesgesetze*] shall be executed by the States

---

<sup>1</sup> The term law is to be understood in the sense of "statute" according to the continental European legal tradition.

<sup>2</sup> The wording refers to the separation of powers under the Austrian Federal Constitution. The Data Protection Commission [*Datenschutzkommission*], as an administrative authority, must not interfere with the workings of the courts or the federal or state legislative assemblies. The restriction does not apply where these organisations act in their capacity as regular administrative authorities, such as when administering their personnel.

unless the execution has been entrusted by federal law to the Data Protection Commission [*Datenschutzkommission*], the Data Protection Council [*Datenschutzrat*] or the courts.

### **Räumlicher Anwendungsbereich**

**§ 3.** (1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.

(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.

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

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

### **Territorial Jurisdiction**

**Sect. 3** (1) The provisions of this Federal Act [*Bundesgesetz*] shall be applied to the use of personal data in Austria. This Federal Act shall also be applied to the use of data [*Verwendung von Daten*] outside of Austria, insofar as the data is used in other Member States of the European Union for purposes of a main establishment or branch establishment (sect. 4 sub-para. 15) in Austria of the controller [*Auftraggeber*] (sect. 4 sub-para. 4).

(2) Deviating from para. 1 the law of the state where the controller has its seat applies, when a controller of the private sector (sect. 5 para. 3), whose seat is in another Member State of the European Union, uses personal data in Austria for a purpose that cannot be ascribed to any of the controller's establishments in Austria.

(3) Furthermore, this law shall not be applied insofar as data are only transmitted through Austrian territory.

(4) Legal provisions deviating from paras. 1 to 3 shall be permissible only in matters not subject to the jurisdiction of the European Union.

## **Artikel 2**

### **1. Abschnitt - Allgemeines**

#### **Definitionen**

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

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

2. *"sensible Daten"* (*"besonders schutzwürdige Daten"*): Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben;
3. *"Betroffener"*: jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden;
4. *"Auftraggeber"*: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), und zwar unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber;
5. *"Dienstleister"*: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (Z 8);
6. *"Datei"*: strukturierte Sammlung von Daten, die nach mindestens einem Suchkriterium zugänglich sind;
7. *"Datenanwendung"* (*früher: "Datenverarbeitung"*): die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung);
8. *"Verwenden von Daten"*: jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten.
9. *"Verarbeiten von Daten"*: das Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen (Z 11), Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittels (Z 12) von Daten;
10. *"Ermitteln von Daten"*: das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden;
11. *"Überlassen von Daten"*: die Weitergabe von Daten vom Auftraggeber an einen Dienstleister;
12. *"Übermitteln von Daten"*: die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichende solcher Daten; darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers;
13. *"Informationsverbundsystem"*: die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, daß jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden;
14. *"Zustimmung"*: die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, daß er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt;



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

## Article 2

### Part 1 - General Provisions

#### Definitions

**Sect. 4.** For the subsequent provisions of this Federal Act [*Bundesgesetz*] the terms listed below shall mean:

1. "*Data*" ("*Personal Data*") [*Daten*] ("*personenbezogene Daten*"): Information relating to data subjects (sub-para. 3) who are identified or identifiable; Data are "only indirectly personal" for a controller (sub-para. 4), a processor (sub-para. 5) or recipient of a transmission (sub-para. 12) when the Data relate to the subject in such a manner that the controller, processor or recipient of a transmission cannot establish the identity of the data subject by legal means;
2. "*Sensitive Data*" ("*Data deserving special protection*") [*sensible Daten*] ("*besonders schutzwürdige Daten*"): Data relating to natural persons concerning their racial or ethnic origin, political opinion, trade-union membership, religious or philosophical beliefs, and data concerning health or sex life;
3. "*Data Subject*" [*Betroffener*]: any natural or legal person or group of natural persons not identical with the controller, whose data are processed (sub-para. 8);
4. "*Controller*" [*Auftraggeber*]: natural or legal person, group of persons or organ of a territorial corporate body [*Gebietskörperschaft*] <sup>3</sup> or the offices<sup>4</sup> of these organs, if they decide alone or jointly with others to process data for a specific purpose (sub-para. 9), without regard whether they do the processing themselves or have it done by somebody else. The above-mentioned persons, group of persons or institutions are also deemed to be processors when they give Data to somebody else for a commissioned work and that person decides to process these Data. If the contractor [*Auftragnehmer*] was expressly prohibited to process the Data when he received the commission or if the contractor himself has to decide on the use, in particular whether to process the committed data, pursuant to legal provisions, professional rules or codes of conduct according to sect. 6 para. 4, he is regarded as the controller;
5. "*Processor*" [*Dienstleister*]: natural or legal person, group of persons or organ of a federal, state and local authority [*Gebietskörperschaft*] or the offices of these organs, who process data that were given to them for a commissioned work (sub-para. 8);
6. "*Filing System*"<sup>5</sup> [*Datei*]: structured set of personal data which are accessible according to at least one specific criterion;
7. "*Data Application*" (former definition: "*electronic data processing*") [*Datenanwendung*] (früher: "*Datenverarbeitung*"): the sum of logically linked stages of data use (sub-para. 8) which are organised in order to reach a defined result (the purpose of the Data Application) and which are as a whole or partially performed automatically, that is, performed by machines and controlled through programs (automated data processing);

---

<sup>3</sup> This is the translation for the word "*Gebietskörperschaft*". It encompasses the federation [*Bund*], the nine member states [*Länder*, singular *Land*] and the municipalities, towns and villages [*Gemeinden*].

<sup>4</sup> This item refers to a peculiarity of Austria public law. The offices of an organ of a federal, regional and local authority [*Gebietskörperschaft*] may act as controllers.

<sup>5</sup> The German word "*Datei*", which is used in the original text, can also mean "file" in the sense of a computer file (The "file" menu of many modern computer programs is called "*Datei*" in German versions), but refers to a filing system in this context.

8. "Use of Data" ["Verwenden von Daten"]: all kinds of operations with Data of a Data Application, meaning both processing of data (sub-para. 9) and transmission of Data (sub-para. 12);
9. "Processing of Data" ["Verarbeiten von Daten"]: the collection, recording, storing, sorting, comparing, modification, interlinkage, reproduction, consultation, output, utilisation, committing (No. 11), blocking, erasure or destruction or any other kind of operation with data of a data application by the controller or processor except the transmission of Data (sub-para. 12);
10. "Collection of Data" ["Ermitteln von Daten"]: The acquisition of data with the intention of using them in a data application;
11. "Committing of Data" ["Überlassen von Daten"]: the transfer of data from the controller to a processor;
12. "Transmission of Data" ["Übermitteln von Daten"]: the transfer of data of a data application to recipients other than the data subject, the controller or a processor, in particular publishing of such data as well as the use of data for another application purpose [Aufgabengebiet] of the controller;
13. "Joint Information System" ["Informationsverbundsystem"]: joint processing of data in a data application by several controllers and the joint utilisation of the data so that every controller has access even to those data in the system that have been made available to the system by other controllers;
14. "Consent" ["Zustimmung"]: the valid declaration of intention of the data subject, given without constraint, that he agrees to the use of data relating to him in a given case, after having been informed about the prevalent circumstances;
15. "Establishment" ["Niederlassung"]: any organisational unit set apart in terms of layout and function by fixed facilities at a specific place, with or without the status of a legal person, which carries out activities at the place where it is set up.

### **Öffentlicher und privater Bereich**

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

- (2) Auftraggeber des öffentlichen Bereichs sind alle Auftraggeber,
1. die in Formen des öffentlichen Rechts eingerichtet sind, insbesondere auch als Organ einer Gebietskörperschaft, oder
  2. soweit sie trotz ihrer Einrichtung in Formen des Privatrechts in Vollziehung der Gesetze tätig sind.

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

### **Public and Private Sector**

**Sect. 5** (1) Data applications [Datenanwendungen] shall be imputed to the public sector according to this Federal Act [Bundesgesetz] if they are undertaken for purposes of a controller of the public sector (p. 2).

- (2) Public sector controllers are all those controllers who
1. are established according to public law legal structures, in particular also as an organ of a territorial corporate body [Gebietskörperschaft], or
  2. as far as they execute laws despite having been incorporated according to private law.

(3) Controller not within the scope of para. 2 are considered controllers of the private sector according to this Federal Act [Bundesgesetz].

## **2. Abschnitt - Verwendung von Daten**

### **Grundsätze**

#### **§ 6. (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 oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 zulässig;
3. soweit sie für den Zweck der Datenanwendung wesentlich sind, verwendet werden und über diesen Zweck nicht hinausgehen;
4. so verwendet werden, daß sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind;
5. solange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist; eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

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

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

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

## **Part 2 - Use of Data**

### **Principles**

#### **Sect. 6. (1) Data shall only**

1. be used fairly and lawfully;
2. be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further uses for scientific and statistical purposes is permitted subject to sect. 46 and 47;
3. be used insofar as they are essential for the purpose of the data application [*Datenanwendung*] and are not excessive in relation to the purpose;
4. be used so that the results are factually correct with regard to the purpose of the application, and the data must be kept up to date when necessary;
5. be kept in a form which permits identification of data subjects [*Betroffene*] as long as this is necessary for the purpose for which the data were collected; a longer period of storage may be laid down in specific laws, particularly laws concerning archives.

(2) The controller [*Auftraggeber*] shall bear the responsibility that the principles of para. 1 are complied with in all his data applications; this also applies when he employs a processor [*Dienstleister*] to use the data.

(3) A controller responsible for a use of data [*Datenverwendung*] subject to this Federal Act [*Bundesgesetz*] who does not reside in the European Union has to name a representative residing in Austria who can be held responsible in place of the controller, without prejudice to the possibility of legal measures against the controller himself.

(4) To determine more closely what can be regarded as fair and lawful use of data [*Datenverwendung*] in a specific field, representations of interest established by law, other professional associations and comparable bodies may draw up codes of conduct for the private sector. These codes of conduct shall only be published after they have been submitted to the Federal Chancellor [*Bundeskanzler*] for evaluation, have been evaluated and have been found to be in compliance with the present law.

### **Zulässigkeit der Verwendung von Daten**

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

(2) Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß Abs. 1 zulässigen Datenanwendung stammen und
2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - soweit diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

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

### **Legitimate Use of Data**

**Sect. 7** (1) Data shall be processed only insofar as the purpose and content of the data application [*Datenanwendung*] are covered by the statutory competencies or the legitimate authority of the respective controller and the data subjects' [*Betroffener*] interest in secrecy deserving protection is not infringed.

(2) Data shall only be transmitted if

1. they originate from a legal data application according to para. 1 and
2. the recipient has satisfactorily demonstrated to the transmitting party his statutory competence or legitimate authority with regard to the purpose of the transmission [*Übermittlung*], insofar as it is not beyond doubt, and
3. the interests in secrecy of the data subject deserving protection are not infringed by the purpose and content of the transmission.

(3) The legitimacy of a use of data [*Datenverwendung*] requires that the intervention be carried out only to the extent required, and using the least intrusive of all effective methods and that the principles of sect. 6 be respected.

## **Schutzwürdige Geheimhaltungsinteressen bei Verwendung nichtsensibler Daten**

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

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder
4. überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

(2) Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung solcher Daten gemäß § 28 Widerspruch zu erheben, bleibt unberührt.

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

1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist oder
5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat.

(4) Die Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den Verdacht der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen verstößt – unbeschadet der Bestimmungen des Abs. 2 – nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder
2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder
3. sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Bundesgesetz gewährleistet.

### **Interests in Secrecy Deserving Protection for the Use of Non-Sensitive Data**

**Sect. 8** (1) Interests in secrecy deserving protection pursuant to sect. 1 para. 1 are not infringed when using non-sensitive data if

1. an explicit legal authorisation or obligation to use the data exists; or
2. the data subject [*Betroffener*] has given his consent, which can be revoked at any time, the revocation making any further use of the data illegal; or
3. vital interests of the data subject require the use; or
4. overriding legitimate interests pursued by the controller [*Auftraggeber*] or by a third party require the use of data [*Datenverwendung*].

(2) The use of legitimately published data and only indirectly personal data shall not constitute an infringement of interests in secrecy deserving protection. The right to object to the use of such data pursuant to sect. 28 remains unaffected.

(3) Interests in secrecy deserving protection are not infringed according to para. 1 sub-para. 4, in particular if the use of data

1. is an essential requirement for a controller of the public sector to exercise a legally assigned function or
2. is performed by a controller of the public sector in fulfilment of his obligation to provide inter-authority assistance<sup>6</sup> or
3. is required to protect the vital interests of a third party or
4. is necessary for the fulfilment of a contract between the controller and the data subject or
5. is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and if the data were collected legitimately or
6. concerns solely the exercise of a public office by the data subject.

(4) The use of data concerning acts and omissions punishable by the courts or administrative authorities, and in particular concerning suspected criminal offences, as well as data concerning criminal convictions and preventive measures does not - without prejudice to para. 2 - infringe interests in secrecy deserving protection if

1. an explicit legal obligation or authorisation to use the data exists; or
2. the use of such data is an essential requirement for a controller of the public sector to exercise a legally assigned function;
3. the legitimacy of the data application [*Datenanwendung*] otherwise follows from statutory responsibilities or other legitimate interests of the controller that override the data subjects' interests in secrecy deserving protection and the manner of use safeguards the interests of the data subject according to this Federal Act [*Bundesgesetz*].

## **Schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten**

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

1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
2. die Daten in nur indirekt personenbezogener Form verwendet werden oder
3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder
4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder
5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder

---

<sup>6</sup> The term "inter-authority assistance" was used here to translate the German word "Amtshilfe", which stands for the obligation of governmental offices to assist each other on request. Amtshilfe is extensively regulated and well defined; see Federal Chancellery (Editor), Public Administration in Austria (1992) p. 385 (Glossary).

6. der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder
7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
9. die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46 oder zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 verwendet werden oder
11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse im Hinblick auf die Datenverwendung unberührt bleiben, oder
12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder -behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder
13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hierbei 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.

### **Interests in Secrecy Deserving Protection for the Use of Sensitive Data**

**Sect. 9** (1) The use of sensitive data does not infringe interests in secrecy deserving protection only and exclusively if

1. the data subject [*Betroffener*] has obviously made public the data himself or
2. the data are used only in indirectly personal form or
3. the obligation or authorisation to use the data is stipulated by laws, insofar as these serve an important public interest, or
4. the use is made by a controller of the public sector in fulfilment of his obligation to give inter-authority assistance or
5. data are used that concern solely the exercise of a public office by the data subject or
6. the data subject has unambiguously given his consent, which can be revoked at any time, the revocation making any further use of the data illegal, or
7. the processing or transmission [*Übermittlung*] is in the vital interest of the data subject and his consent cannot be obtained in time or
8. the use is in the vital interest of a third party or
9. the use is necessary for establishment, exercise or defence of legal claims of the controller before a public authority and the data were collected legitimately or
10. data are used for private purposes pursuant to sect. 45 or for scientific research or statistics pursuant to sect. 46 or to inform and question the data subject pursuant to sect. 47 or

11. the use is required according to the rights and duties of the controller in the field of employment law and civil service regulations<sup>7</sup> and, and is legitimate according to specific legal provisions; the rights of the labour councils according to the Arbeitsverfassungsgesetz<sup>8</sup> with regard to the use of data [*Datenverwendung*] remain unaffected, or
12. the data are required for the purposes of preventive medicine, medical diagnosis, the provision of health care or treatment or the management of health-care services, and the use of data is performed by medical personnel or other persons subject to an equivalent duty of secrecy, or
13. non-profit-organisations with a political, philosophical, religious or trade-union aim process data revealing the political opinion or philosophical beliefs of natural persons in the course of their legitimate activities, as long as these are data of members, sponsors or other persons who display an interest in the aim of the organisation on a regular basis; these data shall not be disclosed to a third party without the consent of the data subjects unless otherwise provided for by law.

### **Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen**

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

(2) Die beabsichtigte Heranziehung eines Dienstleisters durch einen Auftraggeber des öffentlichen Bereichs im Rahmen einer Datenanwendung, die der Vorabkontrolle gemäß § 18 Abs. 2 unterliegt, ist der Datenschutzkommission mitzuteilen, es sei denn, daß die Inanspruchnahme des Dienstleisters auf Grund ausdrücklicher gesetzlicher Ermächtigung erfolgt oder als Dienstleister eine Organisationseinheit tätig wird, die mit dem Auftraggeber oder einem diesem übergeordneten Organ in einem Über- oder Unterordnungsverhältnis steht. Kommt die Datenschutzkommission zur Auffassung, daß die geplante Inanspruchnahme eines Dienstleisters geeignet ist, schutzwürdige Geheimhaltungsinteressen der Betroffenen zu gefährden, so hat sie dies dem Auftraggeber unverzüglich mitzuteilen. Im übrigen gilt § 30 Abs. 6 Z 4.

### **Legitimate Committing of Data for Service Processing**

**Sect. 10** (1) Controllers [*Auftraggeber*] may employ processors [*Dienstleister*] for their data applications [*Datenanwendungen*] insofar as the latter sufficiently warrant the legitimate and secure use of data [*Datenverwendung*]. The controller shall enter into agreements with the processor necessary therefor and satisfy himself that the agreements are complied with by acquiring the necessary information about the actual measures implemented by the processor.

(2) A planned enlistment of a processor by a controller of the public sector for a data application subject to prior checking [*Vorabkontrolle*] pursuant to sect. 18 para. 2 shall be notified to the Data Protection Commission [*Datenschutzkommission*] unless the enlistment of the processor is carried out on grounds of an explicit legal authorisation or the processor is an organisational unit that is superior or subordinate to the processor or one of his superior organs. The Data Protection Commission shall inform the controller without delay if it comes to the conclusion that the planned enlistment of a

---

<sup>7</sup> The expression "Gebiet des Arbeits- oder Dienstrechts" encompasses both the employment law of the private sector (called *Arbeitsrecht*) and the civil service regulations of the public sector (called *Dienstrecht*).

<sup>8</sup> Art. 96 and 96a Arbeitsverfassungsgesetz, Federal Law Gazette Nr. 22/1974 regulate the rights of labour councils concerning data use, workplace surveillance, etc.



processor may endanger interest in secrecy of the data subject [*Betroffener*] deserving protection. Sect. 30 para. 6 sub-para. 4 applies.

### **Pflichten des Dienstleisters**

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

1. die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden; insbesondere ist die Übermittlung der verwendeten Daten ohne Auftrag des Auftraggebers verboten;
2. alle gemäß § 14 erforderlichen Datensicherheitsmaßnahmen zu treffen; insbesondere dürfen für die Dienstleistung nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datengeheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen;
3. weitere Dienstleister nur mit Billigung des Auftraggebers heranzuziehen und deshalb den Auftraggeber von der beabsichtigten Heranziehung eines weiteren Dienstleisters so rechtzeitig zu verständigen, daß er dies allenfalls untersagen kann;
4. – sofern dies nach der Art der Dienstleistung in Frage kommt – im Einvernehmen mit dem Auftraggeber die notwendigen technischen und organisatorischen Voraussetzungen für die Erfüllung der Auskunfts-, Richtigstellungs- und Löschungspflicht des Auftraggebers zu schaffen;
5. nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten;
6. dem Auftraggeber jene Informationen zur Verfügung zu stellen, die zur Kontrolle der Einhaltung der unter Z 1 bis 5 genannten Verpflichtungen notwendig sind.

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

### **Obligations of the Processor**

**Sect. 11** (1) Irrespective of contractual obligations, all processors [*Dienstleister*] have the following obligations when using data for a controller [*Auftraggeber*]:

1. to use data only according to the instructions of the controller; in particular, the transmission [*Übermittlung*] of the data used is prohibited unless so instructed by the controller;
2. to take all required safety measures pursuant to sect. 14; in particular to employ only operatives who have committed themselves to confidentiality vis-à-vis the processor or are under a statutory obligation of confidentiality;
3. to enlist another processor only with the permission of the controller and therefore to inform the controller of this intended enlistment of another processor in such a timely fashion that the controller has the possibility to object;
4. - insofar as this is possible given the nature of the service processing [*Dienstleistung*] - to create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to grant the right of information, rectification and erasure;
5. to hand over to the controller after the end of the service processing all results of processing and documentation containing data or to keep or destroy them on his request;
6. to make available to the controller all information necessary to control the compliance with the obligations according to sub-paras. 1 to 5.

(2) Agreements between the controller and the processor concerning the details of the obligations according to para. 1 shall be laid down in writing to perpetuate the evidence;

## **Genehmigungsfreie Übermittlung und Überlassung von Daten in das Ausland**

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

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

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

1. die Daten im Inland zulässigerweise veröffentlicht wurden oder
2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden oder
3. die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder
4. Daten aus Datenanwendungen für private Zwecke (§ 45) oder für publizistische Tätigkeit (§ 48) übermittelt werden oder
5. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat oder
6. ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann oder
7. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden, oder
8. die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2 Z 6) oder Musterverordnung (§ 19 Abs. 2) ausdrücklich angeführt ist oder
9. es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt oder
10. Übermittlungen oder Überlassungen aus Datenanwendungen erfolgen, die gemäß § 17 Abs. 3 von der Meldepflicht ausgenommen sind.

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

1. zur Wahrung eines wichtigen öffentlichen Interesses oder
2. zur Wahrung eines lebenswichtigen Interesses einer Person

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

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

## Transborder<sup>9</sup> Transmission and Committing of Data not Subject to Licensing

**Sect. 12** (1) The transmission [*Übermittlung*] and committing [*Überlassung*] of data to recipients in member states of the European Union is not subject to any restrictions in terms of sect. 13. This does not apply to data exchange between public sector controllers [*Auftraggeber*] in fields that are not subject to the law of the European Union.

(2) No authorisation pursuant to sect. 13 shall be required for data exchange with recipients in third countries with an adequate level of data protection. The countries that have an adequate level of data protection shall be enumerated in an ordinance [*Verordnung*] of the Federal Chancellor [*Bundeskanzler*] in accordance with sect. 55 sub-para. 1<sup>10</sup>. The decisive consideration as to the adequacy of the protection shall be the implementation of the principles of sect. 6 para. 1 in the foreign legal system as well as the existence of effective guarantees for their enforcement.

(3) Furthermore, transborder data exchange shall not require authorisation if

1. the data have been published legitimately in Austria or
2. data are transferred or committed that are only indirectly personal to the recipient or
3. the transborder transmission or committing is authorised by regulations that are equivalent to a statute in the Austrian legal system and are immediately applicable or
4. data from a data application [*Datenanwendung*] for private purposes (sect. 45) or for journalistic purposes (sect. 48) is transmitted or
5. the data subject [*Betroffener*] has without any doubt given his consent to the transborder transmission or committing or
6. a contract between the controller and the data subject or a third party that has been concluded clearly in the interest of the data subject cannot be fulfilled except by the transborder transmission of data or
7. the transmission is necessary for the establishment, exercise or defence of legal claims before a foreign authority and the data were collected legitimately or
8. the transmission or committing is expressly named in a standard ordinance [*Standardverordnung*] (sect. 17 para. 2 sub-para. 6) or model ordinance [*Musterverordnung*] (sect. 19 para. 2) or
9. the data exchange is with Austrian governmental missions and offices in foreign countries or
10. the transmissions or commitments are made from a data application that is exempted from notification according to sect. 17 para. 3.

(4) If the transborder transmission or committing in cases not covered by the preceding paragraphs is necessary

1. to safeguard an important public interest or
2. to safeguard a vital interest of a person

and of such urgency that the authorisation of the Data Protection Commission [*Datenschutzkommission*] required according to sect. 13 cannot be obtained in time without risk to the above-mentioned interests, it may be performed without a permit, but must be notified to the Data Protection Commission immediately.

(5) The legality of a data application in Austria according to sect. 7 is a prerequisite for every transborder transmission or committing. Furthermore, transborder commitments require the written promise of the processor [*Dienstleister*] abroad to the domestic controller - or in the case of sect. 13 para. 5 to the domestic processor - that he shall respect the obligations of a processor according to

---

<sup>9</sup> The German word "Ausland" refers to all foreign countries outside of Austria. The term is difficult to translate and has been replaced by the more common word "Transborder".

<sup>10</sup> Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutz-angemessenheits-Verordnung - DSAV), Federal Law Gazette II Nr. 521/1999.

sect. 11 para. 1. This is not applicable if the processing abroad is provided for in regulations that are equivalent to a law in the Austrian legal system and are immediately applicable.

## **Genehmigungspflichtige Übermittlung und Überlassung von Daten ins Ausland**

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

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

1. für die im Genehmigungsantrag angeführte Übermittlung oder Überlassung im konkreten Einzelfall angemessener Datenschutz besteht; dies ist unter Berücksichtigung aller Umstände zu beurteilen, die bei der Datenverwendung eine Rolle spielen, wie insbesondere die Art der verwendeten Daten, die Zweckbestimmung sowie die Dauer der geplanten Verwendung, das Herkunfts- und das Endbestimmungsland und die in dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen, Standesregeln und Sicherheitsstandards; oder
2. der Auftraggeber glaubhaft macht, daß die schutzwürdigen Geheimhaltungsinteressen der vom geplanten Datenverkehr Betroffenen auch im Ausland ausreichend gewahrt werden. Hiefür können insbesondere auch vertragliche Zusicherungen des Empfängers an den Antragsteller über die näheren Umstände der Datenverwendung im Ausland von Bedeutung sein.

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

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

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

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

(7) Hat der Bundeskanzler trotz Fehlens eines im Empfängerstaat generell geltenden angemessenen Schutzniveaus durch Verordnung festgestellt, daß für bestimmte Kategorien des Datenverkehrs mit diesem Empfängerstaat die Voraussetzungen gemäß Abs. 2 Z 1 zutreffen, tritt an die Stelle der Verpflichtung zur Einholung einer Genehmigung die Pflicht zur Anzeige an die Datenschutzkommission. Die Datenschutzkommission hat binnen sechs

Wochen ab Einlangen der Anzeige mit Bescheid den angezeigten Datenverkehr zu untersagen, wenn er keiner der in der Verordnung geregelten Kategorien zuzurechnen ist oder den Voraussetzungen gemäß § 12 Abs. 5 nicht entspricht; andernfalls ist die Übermittlung oder Überlassung der Daten in das Ausland zulässig.

### **Transborder Transmission and Committing of Data Subject to Licensing**

**Sect. 13** (1) Insofar as a case of transborder data exchange is not exempted from authorisation according to sect. 12, the controller has to apply for a permit by the Data Protection Commission [*Datenschutzkommission*] (sect. 35) before the transmission [*Übermittlung*] or committing [*Überlassung*]. The Data Protection Commission can issue the permit subject to conditions and obligations.

(2) The permit shall be given, taking into consideration the promulgations [*Kundmachungen*] pursuant to sect. 55 sub-para. 2, if the requirements of sect. 12 para. 5 are met, and despite the lack of an adequate general level of data protection in the recipient state

1. an adequate level of data protection exists for the transmission or committing outlined in the application for the permit in this specific case; this is then to be judged considering all circumstances relevant to the use of data [*Datenverwendung*], such as the type of data used, the purpose and duration of use, the country of origin and final destination as well as the general and sectoral legal provisions, professional rules and security standards applying in the third country; or
2. the controller can satisfactorily demonstrate that the interests in secrecy deserving protection of the data subject [*Betroffener*] of the planned data exchange will be respected outside of Austria. In particular, contractual guarantees by the recipient to the applicant about the circumstances of the use of data are significant for the decision.

(3) Controllers of the public sector shall enjoy the rights of a party to the proceedings for issue of a permit, even with regard to the data applications [*Datenanwendungen*] they perform to in execution of the law<sup>11</sup>.

(4) In the case of data applications subject to notification, the Data Protection Commission shall put a copy of each ruling [*Bescheid*] authorising the transborder transmission or committing of data on the notification file<sup>12</sup> and enter the fact that authorisation has been granted into the Data Processing Register [*Datenverarbeitungsregister*] (sect. 16).

(5) Deviating from para. 1, a domestic processor [*Dienstleister*] can apply for a permit if, in order to fulfil his contractual duties vis-à-vis multiple controllers, he wishes to enlist the service of a specific processor outside of Austria. The actual committing shall only be performed with the consent of the controller. The controller shall report to the Data Protection Commission from which of his data applications subject to notification the authorised committing to the processor shall take place; this is to be entered into the Data Processing Register.

(6) The transmission of data to representations of foreign governments or intergovernmental institutions in Austria shall be treated as transborder data exchange with regard to the requirement for authorisation according to para. 1.

(7) If the Federal Chancellor [*Bundeskanzler*] has decreed by ordinance [*Verordnung*] that, despite the lack of an adequate general level of data protection in the recipient state, the requirements according to para. 2 sub-para. 1 are met for specific categories of data exchange with this recipient state, the obligation to obtain a permit is replaced by an obligation to notify the Data Protection

---

<sup>11</sup> This is a peculiarity of Austrian law: Public sector controllers do not normally enjoy the rights of a party to the proceedings.

<sup>12</sup> Here, the word "file" means a collection of documents belonging to a specific case.

Commission. The Data Protection Commission shall prohibit the notified data exchange within six weeks after receiving the notification if it is not attributed to one of the categories regulated in the ordinance [*Verordnung*] or if it does not fulfil the requirements according to sect. 12 para. 5; otherwise the transmission or committing is permitted.

### **3. Abschnitt - Datensicherheit**

#### **Datensicherheitsmassnahmen**

**§ 14.** (1) Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Gewährleistung der Datensicherheit zu treffen. Dabei ist je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit sicherzustellen, daß die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, daß ihre Verwendung ordnungsgemäß erfolgt und daß die Daten Unbefugten nicht zugänglich sind.

- (2) Insbesondere ist, soweit dies im Hinblick auf Abs. 1 letzter Satz erforderlich ist,
1. die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ausdrücklich festzulegen,
  2. die Verwendung von Daten an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden,
  3. jeder Mitarbeiter über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren,
  4. die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters zu regeln,
  5. die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte zu regeln,
  6. die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen die unbefugte Inbetriebnahme abzusichern,
  7. Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können,
  8. eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern.

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

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

(4) Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck – das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes – unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung, es sei denn, daß es sich um die Verwendung zum Zweck der Verhinderung oder Verfolgung eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, handelt.

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

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

### **Part 3 - Data Security**

#### **Data Security Measures**

**Sect. 14** (1) Measures to ensure data security shall be taken by all organisational units of a controller [*Auftraggeber*] or processor [*Dienstleister*] that use data. Depending on the kind of data used as well as the extent and purpose of the use and considering the state of technical possibilities and economic justifiability it shall be ensured that the data are protected against accidental or intentional destruction or loss, that they are properly used and are not accessible to unauthorised persons.

(2) In particular, the following measures are to be taken insofar as this is necessary with regard to the last sentence of para. 1:

1. The distribution of functions between the organisational units as well as the operatives regarding the use of data [*Datenverwendung*] shall be laid down expressly,
2. The use of data must be tied to valid orders of the authorised organisational units or operatives,
3. every operative is to be instructed about his duties according to this Federal Act [*Bundesgesetz*] and the internal data protection regulations, including data security regulations,
4. The right of access to the premises of the data controller or processor is to be regulated,
5. The right of access to data and programs is to be regulated as well as the protection of storage media against access and use by unauthorised persons,
6. The right to operate the data processing equipment is to be laid down and every device is to be secured against unauthorised operation by taking precautions for the machines and programs used,
7. Logs shall be kept in order that the processing steps that were actually performed, in particular modifications, consultations and transmissions [*Übermittlungen*], can be traced to the extent necessary with regard to their permissibility,
8. A documentation shall be kept on the measures taken pursuant to sub-paras. 1 to 7 to facilitate control and conservation of evidence.

These measures must, taking into account the technological state of the art and the cost incurred in their execution, safeguard a level of data protection appropriate with regard to the risks arising from the use and the type of data to be protected.

(3) Unregistered transmissions from data applications [*Datenanwendungen*] subject to an obligation to grant information pursuant to sect. 26 shall be logged in such a manner that the right of information [*Auskunftsrecht*] can be granted to the subject pursuant to sect. 26. Transmissions provided for in the standard ordinance [*Standardverordnung*] (sect. 17 para. 2 lit. 6) and the model ordinance [*Musterverordnung*] (sect. 19 para. 2) do not require logging.

(4) Logs and documentation data may not be used for purposes that are incompatible with the purpose of the collection [*Ermittlung*] - viz., monitoring the legitimacy of the use of the logged and documented data files [*Datenbestand*]. In particular, any further use for the purpose of supervising the data subjects [*Betroffener*] whose data is contained in the logged data files, as well as for the purpose of monitoring the persons who have accessed the logged data files, or for any purpose other than checking access rights shall be considered incompatible, unless the data is used is for the purpose of



preventing or prosecuting a crime according to sect. 278a StGB<sup>13</sup> (criminal organisation) or a crime punishable with a maximum sentence of more than five years imprisonment.

(5) Unless expressly provided for otherwise by law, logs and documentation data shall be kept for three years. Deviations from this rule shall be permitted to the same extent that the logged or documented data files [*Datenbestand*] may legitimately be erased earlier or kept longer.

(6) Data security regulations are to be issued and kept available in such a manner that the operatives can inform themselves about the regulations to which they are subject at any time.

## Datengeheimnis

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

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

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

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

## Confidentiality of Data

**Sect. 15** (1) Controllers [*Auftraggeber*], processors [*Dienstleister*] and their operatives - these being the employees and persons comparable to employees - shall keep data from uses of data [*Datenanwendungen*] confidential that have been entrusted or made accessible to them solely for professional reasons, without prejudice to other professional obligations of confidentiality, unless a legitimate reason exists for the transmission [*Übermittlung*] of the entrusted or accessed data (confidentiality of data [*Datengeheimnis*]).

(2) Operatives shall transmit data only if expressly ordered to do so by their employer. controllers and processors shall oblige their operatives by contract, insofar as they are not already obliged by law, to transmit data from uses of data only if so ordered and to adhere to the confidentiality of data even after the end of their professional relationship with the controller or processor.

(3) Controllers and processors may only issue orders for the transmission of data if this is permitted pursuant to the provisions of this Federal Act [*Bundesgesetz*]. They shall inform the operatives affected by these orders about the transmission orders in force and about the consequences of a violation of data confidentiality.

---

<sup>13</sup> StGB: *Strafgesetzbuch* (Penal Code), Federal Law Gazette No. 60/1974.

(4) Without prejudice to the constitutional right to issue instructions [*Weisungen*]<sup>14</sup>, a refusal to follow an order to transmit data on the grounds that it violates the provisions of this Federal Act shall not be to the operatives' detriment.

---

<sup>14</sup> This refers to the right of superiors in administrative authorities to issue instructions.

## **4. Abschnitt - Publizität der Datenanwendungen**

### **Datenverarbeitungsregister**

**§ 16.** (1) Bei der Datenschutzkommission ist ein Register der Datenanwendungen zum Zweck der Prüfung ihrer Rechtmäßigkeit und zum Zweck der Information der Betroffenen eingerichtet.

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

(3) Der Bundeskanzler hat die näheren Bestimmungen über die Führung des Registers durch Verordnung zu erlassen. Dabei ist auf die Richtigkeit und Vollständigkeit des Registers, die Übersichtlichkeit und Aussagekraft der Eintragungen und die Einfachheit der Einsichtnahme Bedacht zu nehmen. Es ist die Möglichkeit vorzusehen, eine Meldung (§§ 17 und 19) auf automationsunterstütztem Wege vorzunehmen.

### ***Part 4 - Publicity of Data Applications***

#### **Data Processing Register**

**Sect. 16** (1) A register for data applications [*Datenanwendungen*] is established with the Data Protection Commission [*Datenschutzkommission*] for the purpose of examining their legality and in order to inform the data subjects [*Betroffene*].

(2) Any person may inspect the register. Access to the registration file including the licences contained therein shall be granted if the person applying for inspection can satisfactorily demonstrate that he is a data subject, and as far as no overriding interest in secrecy on part of the controller deserving protection is an obstacle to access.

(3) The Federal Chancellor [*Bundeskanzler*] shall lay down more specific regulations about the management of the register in an ordinance<sup>15</sup> [*Verordnung*]. This is to be done with due regard to the correctness and completeness of the register, the clarity and expressiveness of the entries and the ease of access. A possibility to notify (sects. 17 and 19) by means of automated processing shall be provided for.

#### **Meldepflicht des Auftraggebers**

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

- (2) Nicht meldepflichtig sind Datenanwendungen, die
1. ausschließlich veröffentlichte Daten enthalten oder
  2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses oder

---

<sup>15</sup> Verordnung des Bundeskanzlers über das bei der Datenschutzkommission eingerichtete Datenverarbeitungsregister (Datenverarbeitungsregister-Verordnung 2002 - DVRV 2002), Federal Law Gazette II Nr. 24/2002

3. nur indirekt personenbezogene Daten enthalten oder
4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) oder
5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden oder
6. einer Standardanwendung entsprechen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

(3) Weiters sind Datenanwendungen für Zwecke

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherstellung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten

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

### **Duty of the Controller to Notify**

**Sect. 17** (1) Every controller [*Auftraggeber*] shall, unless provided for otherwise in paras. 2 and 3, before commencing a data application [*Datenanwendung*], file a notification whose contents are laid down in sect. 19 with the Data Protection Commission [*Datenschutzkommission*] for the purpose of registration in the Data Processing Register [*Datenverarbeitungsregister*]. The duty to notify also applies to all circumstances that subsequently lead to the incorrectness or incompleteness of the notification.

(2) Data applications are not subject to notification

1. which solely contain published data or
2. whose subject is the management of registers and catalogues that are by law open to inspection by the public, even if a legitimate interest for doing so must be demonstrated or
3. which contain only indirectly personal data or
4. which are carried out by natural persons for activities that are entirely personal or concern just the person's family life (sect. 45) or
5. which are carried out for journalistic purposes according to sect. 48 or
6. correspond to a standard application [*Standardanwendung*]. The Federal Chancellor [*Bundeskanzler*] can lay down in an ordinance [*Verordnung*] that some types of data applications and transmissions [*Übermittlung*] are standard applications, if they are carried out by a large number of controllers in similar fashion and if a risk to the data subjects' [*Betroffener*] interest in secrecy deserving protection is unlikely considering the purpose of the use and the processed categories of data [*Datenarten*]. The ordinance shall list for every Standard Application the authorised categories of data, the categories of data subjects [*Betroffenenkreise*] and recipients [*Empfängerkreise*] as well as the maximum period of time during which the data may be stored<sup>16</sup>.

(3) Furthermore, data applications for the purpose of

1. protecting the constitutional institutions of the Republic of Austria or

---

<sup>16</sup> Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2000 - StMV), Federal Law Gazette II Nr. 201/2000.

2. safeguarding the operational readiness of the federal army or
3. safeguarding the interests of comprehensive national defence or
4. protecting important foreign policy, economic or financial interests of the Republic of Austria or the European Union
5. preventing and prosecuting of crimes<sup>17</sup>

shall be exempt from the duty to notify, insofar as this is necessary to achieve the purpose of the data application.

### **Aufnahme der Verarbeitung**

**§ 18.** (1) Der Vollbetrieb einer meldepflichtigen Datenanwendung darf - außer in den Fällen des Abs. 2 - unmittelbar nach Abgabe der Meldung aufgenommen werden.

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

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

erst nach ihrer Prüfung (Vorabkontrolle) durch die Datenschutzkommission nach den näheren Bestimmungen des § 20 aufgenommen werden.

### **Commencement of Processing**

**Sect. 18** (1) A data application [*Datenanwendung*] subject to notification may - except as laid down in para. 2 - take up full operation immediately after the notification has been submitted.

(2) Data applications subject to notification that neither correspond to a Model Application [*Musteranwendung*] pursuant to sect. 19 para. 2 nor concern the internal affairs of the churches and religious communities recognised by the state, and

1. that involve sensitive data or
2. that involve data about offences according to sect. 8 para. 4 or
3. whose purpose is to give information on the data subjects [*Betroffener*] creditworthiness or
4. that are carried out in the form of a joint information system [*Informationsverbundsystem*],

shall be initiated only after an examination (prior checking) [*Vorabkontrolle*] by the Data Protection Commission [*Datenschutzkommission*] in accordance with sect. 20.

### **Notwendiger Inhalt der Meldung**

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

1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 3 oder eines Betreibers gemäß § 50 Abs. 1, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z 2 ergeben, und
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und
5. die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise – einschließlich

---

<sup>17</sup> The two German nouns "Vorbeugung" and "Verhinderung" both mean prevention in English.

allfälliger ausländischer Empfängerstaaten – sowie die Rechtsgrundlagen der Übermittlung und

6. - soweit eine Genehmigung der Datenschutzkommission notwendig ist - die Geschäftszahl der Genehmigung durch die Datenschutzkommission sowie
7. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

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

1. die Bezeichnung der Datenanwendung gemäß der Musterverordnung und
2. die Bezeichnung und Anschrift des Auftraggebers sowie den Nachweis seiner gesetzlichen Zuständigkeit oder seiner rechtlichen Befugnis, soweit dies erforderlich ist, und
3. die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde.

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

### Required Content of the Notification

**Sect. 19** (1) A notification pursuant to sect. 17 must contain

1. the name (or other designation) and address of the controller [*Auftraggeber*] and of his representative according to sect. 6 para. 3 or of the operator pursuant to sect. 50 para. 1; furthermore the registration number of the controller, insofar as one has been already assigned to him, and
2. the proof of statutory competence or of the legitimate authority that the controller's activities are permitted, if so required and
3. the purpose of the data application [*Datenanwendung*] to be registered and the legal basis, as long as this is not included in the information according to sub-para. 2 and
4. the categories of data subjects [*Betroffenenkreise*] and the categories of data [*Datenarten*] about them that are processed and
5. the categories of data subjects [*Betroffenenkreise*] affected by intended transmissions [*Übermittlungen*], the categories of data [*Datenarten*] to be transmitted and the matching categories of recipients [*Empfängerkreise*] - including possible recipient states abroad - as well as the legal basis for the transmission and
6. - insofar as a permit by the Data Protection Commission [*Datenschutzkommission*] is required - the file number of the permit of the Data Protection Commission as well as
7. a general description of data security measures taken pursuant to sect. 14, which enable a preliminary assessment of the appropriateness of the security measures.

(2) If a large number of controllers has to carry out data applications in similar fashion and the prerequisites for a Standard Application [*Standardanwendung*] do not apply, the Federal Chancellor can designate Model Applications [*Musteranwendung*] by ordinance<sup>18</sup> [*Verordnung*]. Notifications of

---

<sup>18</sup> See footnote 16.

data applications whose content corresponds to a Model Application need to contain only the following:

1. the designation of the model application [*Musteranwendung*] according to the model ordinance [*Musterverordnung*] and
2. the designation and address of the controller as well as proof of statutory competencies or of legitimate authority, as far as this is required, and
3. the registration number of the controller, insofar as one has been already assigned to him.

(3) A notification is insufficient if information is missing, obviously incorrect, inconsistent or so insufficient that persons accessing the register to safeguard their rights according to this Federal Act [*Bundesgesetz*] cannot obtain sufficient information as to the issue whether their interests in secrecy deserving protection could be infringed by the data application. In particular, inconsistency is given in case of a deviation of the notified content from the notified legal basis.

### **Prüfungs- und Verbesserungsverfahren**

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

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

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

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

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

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

### **Examination and Correction Procedure**

**Sect. 20** (1) The Data Protection Commission [*Datenschutzkommission*] shall examine all notifications within two month. If the Data Protection Commission comes to the conclusion that the notification is insufficient in terms of sect. 19 para. 3, the controller [*Auftraggeber*] shall be ordered within two month after receipt of the notification to correct the insufficiency within a set period.

(2) In case of imminent danger [*Gefahr im Verzug*] due to a serious infringement of the data subject's interest in secrecy deserving protection, the Data Protection Commission shall temporarily

prohibit by ruling [*Bescheid*] pursuant to sect. 57 AVG<sup>19</sup> the continuation of the notified data application.

(3) For data applications [*Datenanwendungen*] subject to prior checking [*Vorabkontrolle*] pursuant to sect. 18 para. 2, a decision shall be rendered in conjunction with the order for correction stating if processing may be commenced or is not permitted for lack of proving a sufficient legal basis.

(4) If the order for correction is not complied with in a timely manner, the Data Protection Commission shall, by ruling, refuse registration; otherwise the notification shall be regarded as if it had been correct from the beginning.

(5) If no order for correction is made within two month after the notification, the obligation to notify is considered to be fulfilled. Data applications subject to prior checking pursuant to sect. 18 para. 2 may be commenced.

(6) In the registration proceedings, public sector controllers shall have the rights of parties in the registration proceedings even with regard to data applications they carry out in execution of the law.

## Registrierung

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

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

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

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

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

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

## Registration

**Sect. 21** (1) Notifications pursuant to sect. 19 are to be entered into the Data Processing Register [*Datenverarbeitungsregister*] if

1. the checking procedure has shown that a registration is permitted or
2. two months have passed since the notification was submitted to the Data Protection Commission [*Datenschutzkommission*], without a request for correction having been issued pursuant to sect. 20 para. 1 or
3. the controller has made the corrections which were ordered in time.

The information on data security measures contained in the notification shall not be entered into the register.

---

<sup>19</sup> AVG: Allgemeines Verwaltungsverfahrensgesetz 1991 (Law on General Administrative Procedure 1991) Federal Law Gazette No. 51/1991, see e.g. Federal Chancellery (Editor), Public Administration in Austria (1992) p. 385 (Glossary).



(2) For data applications subject to prior checking [*Vorabkontrolle*] pursuant to sect. 18 para. 2, the execution of the data application may be permitted subject to conditions based on the findings of the checking procedure, insofar as this is necessary to safeguard interests of the data subject [*Betroffener*] that are protected by this Federal Act [*Bundesgesetz*].

(3) The successful registration shall be communicated to the controller in writing in the form of a register statement [*Registerauszug*].

(4) A registration number shall be assigned to each controller upon first registration.

### **Richtigstellung des Registers**

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

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

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

(4) Werden der Datenschutzkommission andere als die in Abs. 2 bezeichneten Umstände bekannt, die den Verdacht der Mangelhaftigkeit einer Registrierung im Sinne des § 19 Abs. 3 oder der rechtswidrigen Unterlassung einer Meldung begründen, so hat die Datenschutzkommission ein Verfahren zur Feststellung des für die Erfüllung der Meldepflicht erheblichen Sachverhalts einzuleiten und das Datenverarbeitungsregister entsprechend dem Ergebnis des Verfahrens zu berichtigen.

### **Rectification of the Register**

**Sect. 22** (1) Deletions and amendments to the Data Processing Register [*Datenverarbeitungsregister*] shall be carried out upon application of the registree or ex officio in the cases of para. 2 and 4.

(2) If the Data Protection Commission [*Datenschutzkommission*] learns through official publications about changes in the designation or address of the controller [*Auftraggeber*], the entry shall be corrected ex officio. If an official publication states that the legal basis of the controller [*Auftraggeber*] is no longer valid, the deletion from the register shall be ordered ex officio.

(3) Amendments or deletions pursuant to para. 2 are to be ordered without further investigation by ruling [*Bescheid*].

(4) If the Data Protection Commission learns of circumstances other than those named in para. 2, which give probable cause to believe that a registration is insufficient in terms of sect. 19 para. 3, or of an illegal non-notification, the Data Protection Commission shall initiate an administrative inquiry to determine the relevant circumstances for the fulfilment of the obligation to notify, and shall correct the Data Processing Register according to the findings.

### **Pflicht zur Offenlegung nicht-meldepflichtiger Datenanwendungen**

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

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

### **Obligation to Provide Information on Data Applications not Subject to Notification**

**Sect. 23** (1) Controllers [*Auftraggeber*] of a standard application [*Standardanwendung*] shall inform anyone on request which standard applications they actually carry out.

(2) Data applications not subject to notification shall be disclosed to the Data Protection Commission [*Datenschutzkommission*] in pursuit of its supervisory duties according to sect. 30.

### **Informationspflicht des Auftraggebers**

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

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

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

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

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder
2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder
3. Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne daß dies gesetzlich vorgesehen ist.

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

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

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

### **The Controller's Duty to Provide Information**

**Sect. 24** (1) The controller [*Auftraggeber*] of a data application [*Datenanwendung*] shall inform the data subjects when collecting data in an appropriate manner about

1. the purpose of the data application for which for which the data are collected, and
2. the name and address of the controller,

insofar as this as this information is not already available to the data subject [*Betroffener*], with regard to the particular circumstances of the case.

(2) Information beyond the scope of para. 1 shall be given if this is necessary for fair and lawful processing, in particular if

1. the data subject has a right to object to intended processing or transmission of data pursuant to sect. 28 or
2. it is not clear for the data subject under the circumstances whether he is required by law to reply to the questions posed, or
3. data are to be processed in a joint information system [*Informationsverbundsystem*] that is not authorised by law.

(3) Where data have not been collected by asking the data subject, but through transmission [*Übermittlung*] from another application purpose [*Aufgabengebiet*] of the same controller or from a data application of another controller, the information according to para. 1 may be omitted

1. if the use of data [*Datenverwendung*] is provided for by law or an ordinance [*Verordnung*] or
2. if it is impossible to provide the information because the data subjects cannot be reached or
3. if, considering the improbability of infringements of the data subjects' rights and the expense involved in reaching the data subjects, an unreasonable effort would be required. In particular, this applies if data are collected for purposes of scientific research or statistics pursuant to sect. 46 or address data pursuant to sect. 47 and the requirement to inform the data subject is not explicitly stipulated. The Federal Chancellor may determine further cases by ordinance [*Verordnung*] in which the duty to give information does not apply.

(4) There shall be no duty to provide information regarding such data applications that are not subject to notification pursuant to sect. 17 para. 2 and 3.

### **Pflicht zur Offenlegung der Identität des Auftraggebers**

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

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

### **Obligation to Disclose the Identity of the Controller**

**Sect. 25** (1) In the case of transmissions [*Übermittlungen*] and communications to data subjects [*Betroffene*], the controller [*Auftraggeber*] shall disclose his identity in an appropriate manner, so that the data subjects can pursue their rights. In the case of data application [*Datenanwendung*] subject to notification, communications to the data subject shall carry the controllers registration number.

(2) Where data from a data application are used for purposes of a person other than the controller, without said person receiving a right of disposal and thereby the status of a controller over the used data, the communication to the data subject shall give the identity of the person for whose purposes the data are used as well as the identity of the controller from whose data application the data originate. If this concerns a data application subject to notification, the controller's registration number shall be included in the correspondence. This obligation applies to both the controller and the person in whose name the correspondence to the data subject is communicated.

## **5. Abschnitt - Die Rechte des Betroffenen**

### **Auskunftsrecht**

**§ 26.** (1) Der Auftraggeber hat dem Betroffenen Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hierfür in allgemein verständlicher Form anzuführen. Auf Verlangen des Betroffenen sind auch Namen und Adresse von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Mit Zustimmung des Betroffenen kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) Die Auskunft ist nicht zu erteilen, soweit dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist oder soweit überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten

ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.

(3) Der Betroffene hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß mitzuwirken, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

(4) Innerhalb von acht Wochen nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Betroffene am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen: Es ist in allen Fällen, in welchen keine Auskunft erteilt wird – also auch weil tatsächlich keine Daten verwendet werden –, anstelle einer inhaltlichen Begründung der Hinweis zu geben, daß keine der Auskunftspflicht unterliegenden Daten über den Betroffenen verwendet werden. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen ande-

ren Fällen kann ein pauschalierter Kostenersatz von 18,89 Euro verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

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

(8) Soweit Datenanwendungen von Gesetzes wegen öffentlich einsehbar sind, hat der Betroffene ein Recht auf Auskunft in dem Umfang, in dem ein Einsichtsrecht besteht. Für das Verfahren der Einsichtnahme gelten die näheren Regelungen der das öffentliche Buch oder Register einrichtenden Gesetze.

(9) Für Auskünfte aus dem Strafregister gelten die besonderen Bestimmungen des Strafregistergesetzes 1968 über Strafregisterbescheinigungen.

(10) Im Falle der auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs. 4 eigenverantwortlichen Entscheidung über die Durchführung einer Datenanwendung durch einen Auftragnehmer gemäß § 4 Z 4, dritter Satz, kann der Betroffene sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Betroffenen, soweit dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des eigenverantwortlichen Auftragnehmers mitzuteilen, damit der Betroffene sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann.

## ***Part 5 - Rights of the Data Subject***

### **Right to Information**

**Sect. 26** (1) The controller [*Auftraggeber*] shall provide the data subject [*Betroffener*] with information about the data being processed and relating to him, if the data subject so requests in writing and proves his identity in an appropriate manner. Subject to the agreement of the controller, the request for information can be made orally. The information shall contain the processed data, the available information about their origin, the recipients or categories of recipients [*Empfängerkreise*] of transmissions [*Übermittlungen*], the purpose of the use of data [*Datenverwendung*] as well as its legal basis in an intelligible form. Upon request of the data subject, the names and addresses of processors [*Dienstleister*] shall be disclosed in case they are charged with processing data relating to him. With the consent of the data subject, the information may be provided orally alongside with the possibility to inspect and make duplicates or photocopies instead of being provided in writing.

(2) The information shall not be given insofar as this is essential for the protection of the data subject for special reasons or insofar as overriding legitimate interests pursued by the controller or by a third party, especially overriding public interests, are an obstacle to furnishing the information. Overriding public interests can arise out of the necessity

1. to protect of the constitutional institutions of the Republic of Austria or
2. to safeguard of the operational readiness of the federal army or
3. to safeguard the interests of comprehensive national defence or
4. to protect important foreign policy, economic or financial interests of the Republic of Austria or the European Union or
5. to prevent and prosecute crimes<sup>20</sup>.

---

<sup>20</sup> See footnote 17.

The right to refuse information for the reasons stated in sub-paras. 1 to 5 is subject to control by the Data Protection Commission [*Datenschutzkommission*] pursuant to sect. 30 para. 3 and the special complaint proceeding before the Data Protection Commission pursuant to sect. 31 para. 4.

(3) Upon inquiry, the data subject has to cooperate in the information procedure to a reasonable extent to prevent an unwarranted and disproportionate effort on the part of the controller.

(4) Within eight weeks of the receipt of the request, the information shall be provided or a reason given in writing why the information is not or not completely provided. The information may be refused if the data subject has failed to cooperate in the procedure according to para. 3 or has not reimbursed the cost.

(5) In the areas of the executive responsible for the fields described in para. 2 sub-para. 1 to 5, the procedure in a case where public interests require that no information be given shall be as follows: In all cases where no information is given - even when in fact no data is used - instead of giving a reason in substance, an indication shall be given that no data are being used which are subject to the right to information. The legality of such course of action is subject to review by the Data Protection Commission [*Datenschutzkommission*] pursuant to sect. 30 para. 3 and the special complaint proceeding before the Data Protection Commission pursuant to sect. 31 para. 4.

(6) The information shall be given free of charge if it concerns the current data files [*Datenbestand*] of a use of data and if the data subject has not yet made a request for information to the same controller regarding the same application purpose [*Aufgabengebiet*] in the current year. In all other cases a flat rate compensation of 18,89 Euro may be charged; deviations are permitted to cover actually incurred higher expenses. A compensation already paid shall be refunded, irrespective of any claims for damages, if data have been used illegally or if the information has otherwise led to a correction.

(7) As of the moment the controller has knowledge of a request for information, the controller shall not erase the data relating to the data subject until four months have passed or in case a complaint is lodged with the Data Protection Commission pursuant to sect. 31, until the final conclusion of the proceedings.

(8) Insofar as data applications [*Datenanwendungen*] are by law open to inspection by the public the data subject shall have the right to information to the extent of the right to inspect. The regulations of the law establishing the public record or register shall be applied to the inspection procedure.

(9) For information on Criminal Records [*Strafregister*], the special regulations of the Criminal Records Act 1968 [*Strafregistergesetz 1968*] shall apply.

(10) In case an independent decision about the execution of a data application is made by a contractor [*Auftragnehmer*] pursuant to sect. 4 para. 4 third sentence based on legal provisions, professional rules [*Standesregeln*] and codes of conduct according to sect. 6 para. 4, the data subject may address his request for information to the person undertaking the commissioned work. The aforementioned shall communicate to the data subject, insofar as he does not already know, within two weeks and free of charge, the name and address of the responsible controller so that the data subject can assert his right to information according to para. 1 against that person.

## **Recht auf Richtigstellung oder Löschung**

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

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

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

(2) Der Beweis der Richtigkeit der Daten obliegt - sofern gesetzlich nicht ausdrücklich anderes angeordnet ist - dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

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

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

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in § 26 Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Geheimhaltung erfordern, mit einem Richtigstellungs- oder Löschantrag folgendermaßen zu verfahren: Die Richtigstellung oder Löschung ist vorzunehmen, wenn das Begehren des Betroffenen nach Auffassung des Auftraggebers berechtigt ist. Die gemäß Abs. 4 erforderliche Mitteilung an den Betroffenen hat in allen Fällen dahingehend zu lauten, daß die Überprüfung der Datenbestände des Auftraggebers im Hinblick auf das Richtigstellungs- oder Löschantrag durchgeführt wurde. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

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

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

(9) Die Regelungen der Abs. 1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für öffentliche Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für

1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder
  2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschanträge von Betroffenen
- durch Bundesgesetz nicht anderes bestimmt ist.

### **Right to Rectification and Erasure**

**Sect. 27** (1) Every controller shall rectify or erase data that are incorrect or have been processed contrary to the provisions of this Federal Act [*Bundesgesetz*]

1. on his own, as soon the incorrectness of the data or the inadmissibility of the processing becomes know to him, or
2. on a well-founded application by the data subject [*Betroffener*].

The obligation to rectify data according to sub-para. 1 shall apply only to those data whose correctness is significant for the purpose of the data application [*Datenanwendung*]. The incompleteness of data shall only justify a claim to rectification if the incorrectness, with regard to the purpose of the data application, results in the entire information being incorrect. As soon as data are no longer needed for the purpose of the data application, they shall be regarded as illegally processed data and shall be erased unless their archiving is legally permitted and unless the access to these data is specially secured. Any further use for another purpose shall be legitimate only if a transmission [*Übermittlung*] of the data for this purpose is legitimate; the legitimacy of further uses for scientific or statistical purposes is laid down in sects. 46 and 47.

(2) It shall be the obligation of the controller to prove that the data are correct - unless specifically provided otherwise by law - insofar as the data have not been collected exclusively based on statements made by the data subject.

(3) No rectification or erasure of data is possible insofar as the documentation purpose of a data application does not permit later changes. In such case, the necessary rectifications shall be effected by means of additional comments.

(4) The application for rectification or erasure shall be complied with within eight weeks after receipt and the applicant shall be informed thereof, or a reason in writing shall be given why the requested erasure or rectification was not carried out.

(5) In the areas of the executive responsible for the fields described in sect. 26 para. 2 sub-paras. 1 to 5, the following procedure shall be applied to applications for rectification or erasure, insofar as this is required to safeguard those public interests that require secrecy: The rectification or erasure shall be carried out if the demands of the data subject are justified in the opinion of the controller. The required information pursuant to para. 4 shall in all cases be that a check of the data files [*Datenbestand*] of the controller with regard to the application for rectification or erasure has been performed. The legality of this course of action is subject to review by the Data Protection Commission [*Datenschutzkommission*] according to sect. 30 para. 3 and the special complaint proceeding before the Data Protection Commission pursuant to sect. 31 para. 4.

(6) If the erasure or rectification of data kept solely on media readable by means of automatic processing systems can be carried out only at specific times for economic reasons, the data to be erased shall be kept inaccessible and a correcting remark shall be attached the data that are to be corrected.

(7) If data are used whose correctness is disputed by the data subject, and if neither their correctness or incorrectness can be established, an entry about the dispute [*Bestreitungsvermerk*] shall be attached upon request by the data subject. The entry about the dispute shall be erased only with the



consent of the data subject or on grounds of a decision of the competent court of law or of the Data Protection Commission.

(8) If data that were rectified or erased in terms of para. 1 were transmitted before having been rectified or erased, the controller shall inform the recipient of the data by appropriate means, insofar as this does not constitute an unreasonable effort, in particular with regard to a legitimate interest in the information, and that the recipient can still be determined.

(9) The provisions of para. 1 to 8 shall be applied to the criminal records [*Strafregister*], kept according to the Criminal Records Act 1968 [*Strafregistergesetz 1968*] as well as to public books and registers kept by public sector controllers only insofar as

1. the obligation to rectification and erasure ex officio or
2. the procedure to assert and the competence to decide applications to rectification and erasure of data subjects

is not regulated otherwise by federal law.

### **Widerspruchsrecht**

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

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

### **Right to Object**

**Sect. 28** (1) Insofar as a use of data [*Datenverwendung*] is not authorised by law, every data subject [*Betroffener*] shall have the right to raise an objection with the controller [*Auftraggeber*] of the data application [*Datenanwendung*] against the use of data because of an infringement of an overriding interest in secrecy deserving protection arising from his special situation. If the requirements are met, the controller shall erase the data relating to the data subject within eight weeks from his data application and shall refrain from transmitting the data.

(2) If the inclusion of data in a filing system [*Datei*] open to inspection by the public is not mandated by law, the data subject can object at any time and without any need to give reasons for his application. The data shall be erased within eight weeks.

### **Die Rechte des Betroffenen bei der Verwendung nur indirekt personenbezogener Daten**

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

### **Rights of the Data Subject concerning the Use of only Indirectly Personal Data**

**Sect. 29** The rights granted in sects. 26 to 28 cannot be exercised insofar as only indirectly personal data are used.

## **6. Abschnitt - Rechtsschutz**

### **Kontrollbefugnisse der Datenschutzkommission**

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

(2) Die Datenschutzkommission kann im Fall eines begründeten Verdachtes auf Verletzung der im Abs. 1 genannten Rechte und Pflichten Datenanwendungen überprüfen. Hierbei kann sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in Datenanwendungen und diesbezügliche Unterlagen begehren.

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

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

(5) Informationen, die der Datenschutzkommission oder ihren Beauftragten bei der Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Die Pflicht zur Verschwiegenheit besteht auch gegenüber Gerichten und Verwaltungsbehörden, insbesondere Abgabenbehörden; dies allerdings mit der Maßgabe, daß dann, wenn die Einschau den Verdacht einer strafbaren Handlung nach den §§ 51 oder 52 dieses Bundesgesetzes oder eines Verbrechens nach § 278a StGB (kriminelle Organisation) oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß fünf Jahre übersteigt, ergibt, Anzeige zu erstatten ist und hinsichtlich solcher Verbrechen und Vergehen auch dem Ersuchen der Strafgerichte nach § 26 StPO zu entsprechen ist.

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

1. ein Verfahren zur Überprüfung der Registrierung gemäß § 22 Abs. 4 einleiten, oder
2. Strafanzeige nach §§ 51 oder 52 erstatten, oder
3. bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder
4. bei Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen. Dieses Organ hat innerhalb einer angemessenen, jedoch zwölf Wochen nicht überschreitenden Frist entweder dafür Sorge zu tragen, daß der Empfehlung der Datenschutzkommission entsprochen wird, oder der Datenschutzkommission mitzuteilen, warum der Empfehlung nicht entsprochen wurde. Die Begründung darf von der Datenschutzkommission der Öffentlichkeit in

geeigneter Weise zur Kenntnis gebracht werden, soweit dem nicht die Amtverschwiegenheit entgegensteht.

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

## ***Part 6 - Legal Remedies***

### **Duties of Supervision of the Data Protection Commission**

**Sect. 30** (1) Anyone shall have the right to lodge an application with the Data Protection Commission [*Datenschutzkommission*] because of an alleged infringement of his rights or obligations concerning him pursuant to this Federal Act [*Bundesgesetz*] by a controller [*Auftraggeber*] or processor [*Dienstleister*].

(2) The Data Protection Commission shall have the right to examine data applications [*Datenanwendungen*] in case of reasonable suspicion of an infringement of the rights and obligations mentioned in para. 1. It can order the controller or processor of the examined data application to give all necessary clarifications and to grant access to data applications and relevant documents.

(3) Data applications subject to prior checking [*Vorabkontrolle*] pursuant to sect. 18 para. 2 may be examined without a suspicion of illegal data use. The same applies to those fields of the government where a public sector controller claims that sects. 26 para. 5 and 27 para. 5 are to be applied.

(4) For purposes of the inspection, the Data Protection Commission shall have the right, after having informed the owner of said rooms and the controller (processor), to enter rooms where data applications are carried out, operate data processing equipment, run the processing to be examined and to make copies of the storage media to the extent absolutely required for the exercise of the right to examination. The controller (processor) shall render the assistance necessary for the examination. The supervisory rights are to be exercised in a way that least interferes with the rights of the controller (processor) and third parties.

(5) Information acquired by the Data Protection Commission and its representatives during the examinations shall be used only for supervisory purposes in the context of the execution of data protection regulations. The obligation to confidentiality extends even to courts and administrative authorities, in particular fiscal authorities, with the reservation that, if the examination brings up probable cause to believe that a crime according to sects. 51 and 52 of this Federal Act [*Bundesgesetz*] or a crime according to sect. 278a StGB (criminal organisation) or any crime punishable with more than five years of imprisonment has been committed, a report shall be made and requests for assistance by criminal courts according to sect. 26 StPO<sup>21</sup> regarding such crimes<sup>22</sup> shall be complied with.

(6) To establish the rightful state, the Data Protection Commission can issue recommendations; an appropriate period for compliance shall be set if required. If a recommendation is not obeyed within the set period, the Data Protection Commission shall, depending on the kind of transgression and ex officio,

1. initiate an administrative inquiry to check the registration pursuant to sect. 22 para. 4., or
2. bring a criminal charge pursuant to sects. 51 or 52, or
3. in case of severe transgressions by a private sector controller file a lawsuit before the competent court of law pursuant to sect. 32 para. 5, or

---

<sup>21</sup> StPO: *Strafprozeßordnung 1975* (Code of Criminal Procedure), Federal Law Gazette No. 631/1975.

<sup>22</sup> The German words "*Verbrechen und Vergehen*" refers to a distinction between lesser (*Vergehen*) and more severe crimes (*Verbrechen*).

4. in case of a transgression by an organ of a territorial corporate body [*Gebietskörperschaft*], involve the competent highest authority. This authority shall within an appropriate period, not exceeding twelve weeks, take measures to ensure that the recommendation of the Data Protection Commission is complied with or inform the Data Protection Commission why the recommendation is not complied with. The reason may be publicised by the Data Protection Commission in an appropriate manner as far as not contrary to official secrecy.

(7) The intervening party shall be informed as to how his intervention was dealt with.

### **Beschwerde an die Datenschutzkommission**

**§ 31.** (1) Die Datenschutzkommission erkennt auf Antrag des Betroffenen über behauptete Verletzungen des Rechtes auf Auskunft gemäß § 26 durch den Auftraggeber einer Datenanwendung, soweit sich das Auskunftsbegehren nicht auf die Verwendung von Daten für Akte der Gesetzgebung oder der Gerichtsbarkeit bezieht.

(2) Zur Entscheidung über behauptete Verletzungen der Rechte eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung nach diesem Bundesgesetz ist die Datenschutzkommission dann zuständig, wenn der Betroffene seine Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist.

(3) Bei Gefahr im Verzug kann die Datenschutzkommission im Zuge der Behandlung einer Beschwerde nach Abs. 2 die weitere Verwendung von Daten zur Gänze oder teilweise untersagen oder auch - bei Streitigkeiten über die Richtigkeit von Daten - dem Auftraggeber die Anbringung eines Bestreitungsvermerks auftragen.

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

### **Complaint before the Data Protection Commission**

**Sect. 31** (1) The Data Protection Commission [*Datenschutzkommission*] shall decide on request of the data subject [*Betroffener*] on alleged infringements by the controller [*Auftraggeber*] of a data application [*Datenanwendung*] of the right to information pursuant to sect. 26, insofar as this request for information does not concern a use of data [*Datenverwendung*] for acts of legislation or jurisdiction.

(2) The Data Protection Commission shall be competent to decide on an alleged infringement of the right to secrecy, rectification and erasure of the data subject pursuant to this Federal Act [*Bundesgesetz*] if the data subject has filed a complaint against a public sector controller that is not an organ of legislation or jurisdiction.

(3) In the case of imminent danger [*Gefahr im Verzug*], the Data Protection Commission can, when dealing with a complaint pursuant to para. 2, prohibit all further uses of data entirely or in part or

- in the case of a dispute concerning the correctness of data - order the controller to make an entry about the dispute [*Bestreitungsvermerk*].

(4) If a public sector controller invokes sects. 26 para. 5 or 27 para. 5 vis-à-vis the Data Protection Commission concerning a complaint because of an infringement of the rights to information, rectification and erasure, the Data Protection Commission shall, after having examined the necessity of confidentiality, safeguard the protected public interests during the proceedings. If the Data Protection Commission comes to the conclusion that it was not justified to keep the processed data secret from the data subject, the disclosure of the data shall be ordered by a ruling [*Bescheid*]. The authority against whom action was taken may lodge an appeal against this decision with the administrative court [*Verwaltungsgerichtshof*]. If no such appeal is made and the ruling [*Bescheid*] of the Data Protection Commission is not complied within eight weeks, the Data Protection Commission itself shall carry out the disclosure to the data subject and shall communicate to him the desired information or inform him which data have been rectified or erased.

### **Anrufung der Gerichte**

**§ 32.** (1) Ansprüche gegen Auftraggeber des privaten Bereichs wegen Verletzung der Rechte des Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung sind vom Betroffenen auf dem Zivilrechtsweg geltend zu machen.

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

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

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

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

(6) Die Datenschutzkommission hat, wenn ein Betroffener es verlangt und es zur Wahrung der nach diesem Bundesgesetz geschützten Interessen einer größeren Zahl von Betroffenen geboten ist, einem Rechtsstreit auf Seiten des Betroffenen als Nebenintervenient (§§ 17 ff ZPO) beizutreten.

### **Court Action**

**Sect. 32** (1) Claims against private sector controllers [*Auftraggeber*] for infringements of the right to secrecy, to rectification or erasure shall be brought before the civil courts by the data subject [*Betroffener*].

(2) If data have been used contrary to the provisions of this Federal Act [*Bundesgesetz*], the data subject shall have the right to sue for an end to such unlawful state.

(3) In order to safeguard the legal right to put an end to an unlawful state an injunction may be issued even if the requirements mentioned in sect. 381 EO<sup>23</sup> are not fulfilled. This also applies to orders to make an entry about the dispute [*Bestreitungsvermerk*].

(4) Complaints and applications for injunctions pursuant to this Federal Act shall in the first instance be lodged with the regional civil court [*Landesgericht*] in whose district the data subject has his domicile or seat. The data subject may bring an action before the regional civil court in whose district the controller or processor [*Dienstleister*] has his domicile or seat.

(5) The Data Protection Commission [*Datenschutzkommission*] shall, in a case where there is probable cause to believe that a serious data protection infringement has been committed by a private sector controller, file an action for a declaratory judgement (sect. 228 ZPO<sup>24</sup>) [*Feststellungsklage*] in the court that is competent pursuant to para. 4 second sentence.

(6) On request of a data subject the Data Protection Commission shall, if such action appears necessary to safeguard the protected interests of a large number of data subjects pursuant to this Federal Act, intervene in the proceedings in support of the data subject as an intervening third party [*Nebenintervenient*] (sects. 17 et seq. of the Code of Civil Procedure).

### Schadenersatz

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

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

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

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

### Damages

**Sect. 33** (1) A controller [*Auftraggeber*] or processor [*Dienstleister*] who has culpably used data contrary to the provisions of this Federal Act [*Bundesgesetz*], shall indemnify the data subject [*Betroffener*] pursuant to the general provisions of civil law. If data falling under the categories listed in sect. 18 para. 2 no. 1 to 3 are publicly used in a manner that violates a data subjects' interests in secrecy deserving protection that is suitable to expose that person in a like manner to sect. 7 para. 1 of the Media Act, Federal Law Gazette No. 314/1981, that provision shall be applied even if the public use of data [*Datenverwendung*] is not committed by publication in the media. The claim for

---

<sup>23</sup> EO: *Exekutionsordnung* (Enforcement Proceedings Act), Federal Law Gazette No. 79/1896.

<sup>24</sup> ZPO: *Zivilprozessordnung* (Code of Civil Procedure), Imperial Law Gazette No. 113/1895

appropriate compensation for the defamation suffered shall be brought against the controller of the data used.

(2) The controller or processor shall also be liable for damage caused by their staff, insofar as their actions was casual for the damage.

(3) The controller shall be free from liability if he can prove that the circumstances which caused the damage cannot be attributed to him or his staff (para. 2). This also applies to the exclusion of the processors' liability. In the case of contributory negligence on the part of the injured party or a person for whose conduct the injured party is responsible, sect. 1304 ABGB<sup>25</sup> shall apply.

(4) Lawsuits according to para. 1 shall be brought before the court that is competent according to Sect. 32 para. 4.

### **Gemeinsame Bestimmungen**

**§ 34.** (1) Der Anspruch auf Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32 erlischt, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Dies ist dem Einschreiter im Falle einer verspäteten Eingabe gemäß § 30 mitzuteilen; verspätete Beschwerden nach § 31 und Klagen nach § 32 sind abzuweisen.

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

(3) Ist die vermutete Verletzung schutzwürdiger Geheimhaltungsinteressen eines Betroffenen im Inland gemäß § 3 nach der Rechtsordnung eines anderen Mitgliedstaats der Europäischen Union zu beurteilen, so kann die Datenschutzkommission im Falle ihrer Befassung die zuständige ausländische Datenschutzkontrollstelle um Unterstützung ersuchen.

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

### **Common Provisions**

**Sect. 34** (1) The right to lodge an application according to sect. 30, a complaint according to sect. 31 or legal action according to sect. 32 and claims for damages according to sect. 33 shall apply only if the charge is filed by the intervening party within a year after having gained knowledge of the incident that gave rise to the complaint and no later than three years after the alleged incident. This is to be communicated to the intervening party in the case of a late application according to sect. 30; late complaints according to sect. 31 or legal actions according to sect. 32 shall be dismissed.

(2) Applications according to sect. 30, complaints according to sect. 31 or legal action according to sect. 32 and claims for damages according to sect. 33 can be filed not only because of an alleged infringement of this Federal Act [*Bundesgesetz*], but also based on an infringement of data protection provisions of another member state of the European Union, insofar as these provisions are applicable in Austria according to sect. 3.

(3) If the alleged infringement of a data subjects interest in secrecy deserving protection is to be adjudicated in Austria by applying the national provisions of another member state of the European

---

<sup>25</sup> ABGB: *Allgemeines bürgerliches Gesetzbuch* (Austrian General Civil Code), JGS No. 946/1811

Union pursuant to sect. 3, the Data Protection Commission [*Datenschutzkommission*] shall ask the competent foreign supervisory authority for assistance.

(4) The Data Protection Commission shall render inter-authority assistance [*Amtshilfe*] to the independent supervisory authorities of the member states of the European Union upon request.



## **7. Abschnitt - Kontrollorgane**

### **Datenschutzkommission und Datenschutzrat**

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

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

### **Part 7 - Control Bodies**

#### **Data Protection Commission and Data Protection Council**

**Sect. 35** (1) The Data Protection Commission [*Datenschutzkommission*] and the Data Protection Council [*Datenschutzrat*] shall safeguard data protection in accordance with the regulations of this Federal Act [*Bundesgesetz*] without prejudice to the competence of the Federal Chancellor [*Bundeskanzler*] and the courts of law.

(2) (**Constitutional provision**) The Data Protection Commission shall exercise its functions vis-à-vis the highest executive authorities enumerated in art. 19 B-VG<sup>26</sup>.

#### **Zusammensetzung der Datenschutzkommission**

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

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

1. einen Dreivorschlag des Präsidenten des Obersten Gerichtshofs für das richterliche Mitglied,
2. einen Vorschlag der Länder für zwei Mitglieder,
3. einen Dreivorschlag der Bundeskammer für Arbeiter und Angestellte für ein Mitglied,
4. einen Dreivorschlag der Wirtschaftskammer Österreich für ein Mitglied.

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

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

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

(5) Der Datenschutzkommission können nicht angehören:

1. Mitglieder der Bundesregierung oder einer Landesregierung sowie Staatssekretäre;

---

<sup>26</sup> B-VG: *Bundesverfassungsgesetz* (Federal Constitutional Act), Federal Law Gazette No. 1/1930. The provision says that the highest executive authorities, namely the federal president, the ministers, the secretaries of state and the members of state governments are all subject to the supervisory functions of the Data Protection Commission.

2. Personen, die zum Nationalrat nicht wählbar sind.

(6) Hat ein Mitglied der Datenschutzkommission Einladungen zu drei aufeinanderfolgenden Sitzungen ohne genügende Entschuldigung keine Folge geleistet oder tritt bei einem Mitglied ein Ausschließungsgrund des Abs. 5 nachträglich ein, so hat dies nach seiner Anhörung die Datenschutzkommission festzustellen. Diese Feststellung hat den Verlust der Mitgliedschaft zur Folge. Im übrigen kann ein Mitglied der Datenschutzkommission nur aus einem schwerwiegenden Grund durch Beschluß der Datenschutzkommission, dem mindestens drei ihrer Mitglieder zustimmen müssen, seines Amtes für verlustig erklärt werden. Die Mitgliedschaft endet auch, wenn das Mitglied seine Funktion durch schriftliche Erklärung an den Bundeskanzler zurücklegt.

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

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

### Composition of the Data Protection Commission

**Sect. 36** (1) The Data Protection Commission [*Datenschutzkommission*] shall consist of six members appointed by the Federal President [*Bundespräsident*] on a proposal of the Federal Government [*Bundesregierung*] for a term of five years. Reappointments shall be permitted. All members shall have legal expertise. One member shall be a judge.

(2) The proposal of the Federal Government for the nomination of the members of the Data Protection Commission shall be prepared by the Federal Chancellor. The Federal Chancellor shall choose from

1. a proposal of three candidates by the President of the Supreme Court<sup>27</sup> [*Oberster Gerichtshof*] for the judge,
2. a proposal of the states [*Bundesländer*] for two members,
3. a proposal of three candidates by the Federal Chamber of Labour<sup>28</sup> [*Bundeskammer für Arbeiter und Angestellte*] for one member,
4. a proposal of three candidates by the Austrian Federal Economic Chamber<sup>29</sup> [*Wirtschaftskammer Österreich*] for one member.

All proposed persons should have experience in the field of data protection.

(3) One member shall be proposed from the circle of federal officials with legal expertise.

---

<sup>27</sup> Note that the Supreme Court [*Oberster Gerichtshof*] decides only matters of civil or criminal jurisdiction. There is also the administrative court [*Verwaltungsgerichtshof*], which decides in cases of rulings or action of public authorities, and the constitutional court [*Verfassungsgerichtshof*], which decides complaints based on a claim of unconstitutionality (<http://www.vfgh.gv.at/>). The constitutional court can also declare a law unconstitutional and annul it.

<sup>28</sup> The Vienna branch office is present on the internet: <http://www.akwien.or.at/>.

<sup>29</sup> <http://www.wk.or.at/>

(4) For every regular member an alternate member shall be appointed. The alternate member shall act in case the member is unable to fulfil his duties. The term of the alternate member shall expire with the end of the members term of office; if the term of the member ends prematurely para. 8 shall be applied.

(5) The following persons cannot be members of the Data Protection Commission:

1. members of the Federal Government [*Bundesregierung*] or of a State Government [*Landesregierung*] or Secretaries of State [*Staatssekretäre*];
2. persons who may not be elected for the National Council [*Nationalrat*].

(6) Where a member of the Data Protection Commission fails, without adequate excuse, to take part in three consecutive meetings or if one of the causes for exclusion specified in para. 5 arises after the appointment, the Data Protection Commission shall, after hearing the member concerned, decide on the matter. Such decision shall result in the loss of membership. In all other cases a member of the Data Protection Commission may only be deprived of his office on serious grounds and by a decision of the Data Protection Commission approved by at least three members. The term of office shall end when the member resigns from his function in a written statement to the Federal Chancellor.

(7) Para. 2, 3, 5 and 6 shall be applied to the alternate members the same way as to members.

(8) If membership ends because of death, voluntary resignation or in accordance with para. 6, the respective alternate member (para. 4) shall become a full member of the Data Protection Commission until the expiry of the term of the member he replaced. A new alternate member shall be appointed for that time according to para. 2 and 3. If an alternate member leaves prematurely, a new alternate member shall be appointed without delay.

(9) The members and alternate members of the Data Protection Commission shall be entitled to receive compensation for travel expenses (category 3) according to the regulations for federal officials. They shall furthermore be entitled to a compensation according to the amount of time and effort involved, the amount of which shall be determined in an ordinance<sup>30</sup> of the Federal Government upon request of the Federal Chancellor.

### **Weisungsfreiheit der Datenschutzkommission (Verfassungsbestimmung)**

**§ 37.** (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.

### **Independence of the Data Protection Commission (Constitutional Provision)**

**Sect. 37** (1) The members of the Data Protection Commission [*Datenschutzkommission*] shall be independent and not bound by instructions [*Weisungen*] in the exercise of their duties.

(2) The officials working in the office of the Data Protection Commission shall be bound only by instructions [*Weisungen*] of the chairman and the executive member [*geschäftsführendes Mitglied*] of the Data Protection Commission with regard to their professional work.

---

<sup>30</sup> This is the *Verordnung der Bundesregierung vom 30. September 1980 über die Vergütungen für die Mitglieder der Datenschutzkommission*, Federal Law Gazette No. 427/1980.

## Organisation und Geschäftsführung der Datenschutzkommission

**§ 38. (1) (Verfassungsbestimmung)** Die Datenschutzkommission hat sich eine Geschäftsordnung zu geben, in der eines ihrer Mitglieder mit der Führung der laufenden Geschäfte zu betrauen ist (geschäftsführendes Mitglied). Diese Betrauung umfaßt auch die Erlassung von verfahrensrechtlichen Bescheiden und von Mandatsbescheiden im Registrierungsverfahren gemäß § 20 Abs. 2 oder § 22 Abs. 3. Inwieweit einzelne fachlich geeignete Bedienstete der Geschäftsstelle der Datenschutzkommission zum Handeln für die Datenschutzkommission oder das geschäftsführende Mitglied ermächtigt werden, bestimmt die Geschäftsordnung.

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

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

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

## Organisation and Operation of the Data Protection Commission

**Sect. 38 (1) (Constitutional Provision)** The Data Protection Commission [*Datenschutzkommission*] shall adopt its own rules of procedure, in which one of its members shall be charged with directing the current business (executive member) [*geschäftsführendes Mitglied*]. This shall include rulings [*Bescheide*] on procedure and provisional rulings<sup>31</sup> [*Mandatsbescheide*] in the course of the registration proceedings according to sect. 20 para. 2 and sect. 22 para. 3. Whether competent members of the office of the Data Protection Commission shall be authorised to act on behalf of the Data Protection Commission or the executive member [*geschäftsführendes Mitglied*], shall be laid down in the rules of procedure.

(2) The Federal Chancellor [*Bundeskanzler*] shall install an office and supply the necessary personnel and equipment to support the operation of the Data Protection Commission.

(3) The Data Protection Commission shall be heard before an ordinance based on this Federal Act [*Bundesgesetz*] is enacted or which otherwise directly concerns important issues of data protection.

(4) The Data Protection Commission shall compile a report about its activities at least every other year and publish it in an appropriate manner. The report shall be forwarded to the Federal Chancellor.

## Beschlüsse der Datenschutzkommission

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

(2) Das richterliche Mitglied führt den Vorsitz.

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

---

<sup>31</sup> The German word *Mandatsbescheid* refers to a form of provisional ruling. The right to issue such decisions is limited to small fines and very urgent matters. Tickets for parking violations are a special subcase of *Mandatsbescheid*.

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

### **Decisions of the Data Protection Commission**

**Sect. 39** (1) The Data Protection Commission [*Datenschutzkommission*] shall be able to make decisions when all six members are present. Sect. 36 para. 4 shall apply when a member is unable to fulfil his duties.

(2) The judge shall preside.

(3) A valid decision of the Data Protection Commission shall require a majority of votes cast. In the case of a parity of votes the vote of the chairman shall decide the issue. An abstention from the vote is not permitted.

(4) Decisions of the Data Protection Commission that are of fundamental importance for the general public shall be published in an appropriate manner by the Data Protection Commission taking into account the requirements of official secrecy.

### **Wirkung von Bescheiden der Datenschutzkommission und des geschäftsführenden Mitglieds**

**§ 40.** (1) Gegen Bescheide, die das geschäftsführende Mitglied der Datenschutzkommission gemäß § 20 Abs. 2 oder § 22 Abs. 3 in Verbindung mit § 38 Abs. 1 erlassen hat, ist die Vorstellung an die Datenschutzkommission gemäß § 57 Abs. 2 AVG zulässig. Eine Vorstellung gegen einen gemäß § 22 Abs. 3 ergangenen Bescheid hat aufschiebende Wirkung.

(2) Gegen Bescheide der Datenschutzkommission ist kein Rechtsmittel zulässig. Sie unterliegen nicht der Aufhebung oder Abänderung im Verwaltungsweg. Die Anrufung des Verwaltungsgerichtshofes durch die Parteien des Verfahrens ist außer in den Fällen des Abs. 1 zulässig. Dies gilt auch für die in Vollziehung der Gesetze tätigen Auftraggeber des öffentlichen Bereichs in jenen Fällen, in welchen ihnen gemäß § 13 Abs. 3 oder § 20 Abs. 6 Parteistellung zukommt oder durch Gesetz ausdrücklich ein Beschwerderecht an den Verwaltungsgerichtshof eingeräumt wurde.

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

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

### **Effect of Rulings of the Data Protection Commission and the Executive Member**

**Sect. 40** (1) Rulings [*Bescheide*] of the executive member [*geschäftsführendes Mitglied*] of the Data Protection Commission [*Datenschutzkommission*] pursuant to sect. 20 para. 2 or sect. 22 para. 3

in conjunction with sect. 38 para. 1 are subject to appeal<sup>32</sup> [*Vorstellung*] pursuant to sect. 57 para. 2 AVG. An appeal against a ruling [*Bescheid*] pursuant to sect. 22 para. 3. shall have suspensive effect.

(2) No regular remedy at law shall be permitted against rulings [*Bescheide*] of the Data Protection Commission. They are not subject to repeal or modification by administrative procedure. The parties shall have the right to bring the case before the Administrative Court<sup>33</sup> [*Verwaltungsgerichtshof*] except in the case of para. 1. This also applies to public sector controllers that execute laws in those cases where they enjoy the rights of a party to the proceedings according to sect. 13 para. 3 or sect. 20 para. 6 or whenever the right to lodge a complaint with the Administrative Court has been granted by law.

(3) Rulings permitting the transborder transmission [*Übermittlung*] or committing of data [*Überlassung*] pursuant to sect. 13 shall be cancelled whenever the legal or factual prerequisites for granting a permit no longer apply, in particular as the result of a promulgation [*Kundmachung*] of the Federal Chancellor pursuant to sect. 55.

(4) If the Data Protection Commission has established that an infringement of provisions of this Federal Act [*Bundesgesetz*] by a public sector controller has taken place, said controller shall without delay and with all means at his disposal create the state expressed in the legal opinion of the Data Protection Commission.

## **Einrichtung und Aufgaben des Datenschutzrates**

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

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

1. kann der Datenschutzrat Fragen von grundsätzlicher Bedeutung für den Datenschutz in Beratung ziehen;
2. ist dem Datenschutzrat Gelegenheit zur Stellungnahme zu Gesetzesentwürfen der Bundesministerien zu geben, soweit diese datenschutzrechtlich von Bedeutung sind;
3. haben Auftraggeber des öffentlichen Bereichs ihre Vorhaben dem Datenschutzrat zur Stellungnahme zuzuleiten, soweit diese datenschutzrechtlich von Bedeutung sind;
4. hat der Datenschutzrat das Recht, von Auftraggebern des öffentlichen Bereichs Auskünfte und Berichte sowie die Einsicht in Unterlagen zu verlangen, soweit dies zur datenschutzrechtlichen Beurteilung von Vorhaben mit wesentlichen Auswirkungen auf den Datenschutz in Österreich notwendig ist;
5. kann der Datenschutzrat Auftraggeber des privaten Bereichs oder auch ihre gesetzliche Interessenvertretung zur Stellungnahme zu Entwicklungen von allgemeiner Bedeutung auffordern, die aus datenschutzrechtlicher Sicht Anlaß zu Bedenken, zumindest aber Anlaß zur Beobachtung geben;
6. kann der Datenschutzrat seine Beobachtungen, Bedenken und allfälligen Anregungen zur Verbesserung des Datenschutzes in Österreich der Bundesregierung und den Landesregierungen mitteilen, sowie über Vermittlung dieser Organe den gesetzgebenden Körperschaften zur Kenntnis bringen.

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

---

<sup>32</sup> Note that this is not a regular form of appeal, but a special remedy called "Vorstellung" used in conjunction with the *Mandatsbescheid* (footnote 31). The decision of the executive member is appealed before the Data Protection Commission itself, not a higher authority.

<sup>33</sup> The administrative court is not a "regular remedy" in the context of the system of administrative procedures; hence the first sentence.

## Establishment and Duties of the Data Protection Council

**Sect. 41** (1) A Data Protection Council [*Datenschutzrat*] is<sup>34</sup> established at the Federal Chancellery [*Bundeskanzleramt*].

(2) The Data Protection Council shall advise the Federal Government [*Bundesregierung*] and the State Governments [*Landesregierungen*] on requests in political matters of data protection. For this purpose,

1. the Data Protection Council can deliberate on questions of fundamental importance for data protection;
2. the Data Protection Council shall be given opportunity to give its opinion on draft bills of Federal Ministries [*Bundesministerien*], insofar as these are significant for data protection;
3. public sector controllers shall present their projects to the Data Protection Council for evaluation, insofar as these are significant for data protection;
4. the Data Protection Council shall have the right to request information and documents from public sector controllers insofar as this is necessary to evaluate projects of significant impact on data protection in Austria;
5. the Data Protection Council may ask private sector controllers or their representations of interest established by law to give their opinion on developments of general importance that give cause for concern or at least call for attention from a data protection perspective;
6. the Data Protection Council may transmit its observations, concerns and suggestions for improvements of data protection in Austria to the Federal Government and the State Governments, as well as to the legislative bodies by way of these organs.

(3) Para. 2 sub-paras. 3 and 4 shall not apply insofar as the internal affairs of the churches and religious communities recognised by law are concerned.

## Zusammensetzung des Datenschutzrates

**§ 42.** (1) Dem Datenschutzrat gehören an:

1. Vertreter der politischen Parteien: Von der im Hauptausschuß des Nationalrates am stärksten vertretenen Partei sind vier Vertreter, von der am zweitstärksten vertretenen Partei sind drei Vertreter und von jeder anderen im Hauptausschuß des Nationalrates vertretenen Partei ist ein Vertreter in den Datenschutzrat zu entsenden. Bei Mandatsgleichheit der beiden im Nationalrat am stärksten vertretenen Parteien entsendet jede dieser Parteien drei Vertreter;
2. je ein Vertreter der Bundeskammer für Arbeiter und Angestellte und der Wirtschaftskammer Österreich;
3. zwei Vertreter der Länder;
4. je ein Vertreter des Gemeindebundes und des Städtebundes;
5. ein vom Bundeskanzler zu ernennender Vertreter des Bundes.

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

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

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

(5) Die Mitglieder gehören dem Datenschutzrat solange an, bis sie dem Bundeskanzler schriftlich ihr Ausscheiden mitteilen oder, mangels einer solchen Mitteilung, von der

---

<sup>34</sup> The Data Protection Council is already established; therefore, the wording in both German and English merely confirms its existence.

entsendenden Stelle (Abs. 1) dem Bundeskanzler ein anderer Vertreter namhaft gemacht wird.

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

### **Composition of the Data Protection Council**

**Sect. 42** (1) The Data Protection Council [*Datenschutzrat*] shall have the following members:

1. representatives of the political parties: The party that is most strongly represented in the Main Committee of the National Council [*Hauptausschuß des Nationalrates*] shall delegate four representatives, the second strongest shall delegate three members and all other parties represented in the Main Committee of the National Council shall delegate one member each. If the two parties that are most strongly represented in the National Council [*Nationalrat*] have an equal number of seats, each of said parties shall delegate three members;
2. one representative each from Federal Chamber of Labour [*Bundeskammer für Arbeiter und Angestellte*] and the Austrian Federal Economic Chamber [*Wirtschaftskammer Österreich*];
3. two representatives of the States [*Länder*];
4. one representative each of the Association of Austrian Municipalities [*Gemeindebund*] and the Austrian Association of Towns [*Städtebund*];
5. a member of the Federation [*Bund*] appointed by the Federal Chancellor [*Bundeskanzler*].

(2) The representatives mentioned in para. 1 sub-para. 3, 4 and 5 should have professional experience in the field of computer science and data protection.

(3) An alternate representative shall be nominated for every representative.

(4) Members of the Federal Government [*Bundesregierung*] or of a State Government [*Landesregierung*] or Secretaries of State [*Staatssekretäre*] as well as persons who may not be elected for the National Council [*Nationalrat*] shall not be members of the Data Protection Council [*Datenschutzrat*].

(5) The representatives shall be members of the Data Protection Council until they announce their resignation in writing to the Federal Chancellor [*Bundeskanzler*], or, if no resignation is announced, until the nominating body (para. 1) has named another representative to the Federal Chancellor.

(6) The members of the Data Protection Council shall serve in an honorary capacity. Members of the Data Protection Council living outside of Vienna shall be entitled to receive compensation for travel expenses (category 3) according to the regulations for federal officials, if they attend meetings of the Data Protection Council.

### **Vorsitz und Geschäftsführung des Datenschutzrates**

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

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

(3) Die Geschäftsführung des Datenschutzrates obliegt dem Bundeskanzleramt. Der Bundeskanzler hat das hierfür 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.



## **Chairmanship and Operation of the Data Protection Council**

**Sect. 43** (1) The Data Protection Council shall decide on its rules of procedure.

(2) The Data Protection Council [*Datenschutzrat*] shall elect a chairman and two vice chairmen. The term of office of the chairman and the vice chairmen shall be five years, without prejudice to sect. 42 para. 5. Reappointments shall be permitted.

(3) The Federal Chancellery [*Bundeskanzleramt*] shall be responsible for the operation of the Data Protection Council. The Federal Chancellor [*Bundeskanzler*] shall supply the necessary personnel. While working for the Data Protection Council, the officials of the Federal Chancellery shall be bound only by instructions [*Weisungen*] of the chairman of the Data Protection Council with regard to their professional work.

## **Sitzungen und Beschlußfassung des Datenschutrates**

**§ 44.** (1) Die Sitzungen des Datenschutrates 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 Datenschutrat 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. Die Beifügung von Minderheitenvoten ist zulässig.

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

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

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

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

(8) Die Mitglieder des Datenschutrates, 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 Datenschutrat bekanntgewordenen Tatsachen verpflichtet, sofern die Geheimhaltung im öffentlichen Interesse oder im Interesse einer Partei geboten ist.

## **Meetings and Decisions of the Data Protection Council**

**Sect. 44** (1) The meeting of the Data Protection Council [*Datenschutzrat*] shall be convened by the chairman whenever the need arises. If a member requests that a meeting be convened, the chairman shall convene the meeting so that it can take place within four weeks.

(2) The chairman can bring experts into the meeting whenever the need arises.

(3) Deliberations and decisions of the Data Protection Council shall require the presence of at least half of its members. Decisions shall be passed by a simple majority of votes cast. In the case of a parity of votes, the vote of the chairman shall decide the issue. An abstention from the vote is not permitted. A dissenting opinion may be given.

(4) The Data Protection Council may create permanent or ad hoc working groups which it may entrust with the preparation, appraisal and handling of specific issues. An individual member (rapporteur) may be entrusted with executive work, the first appraisal and handling of specific issues.

(5) Every member of the Data Protection Council must - except in case of justifiably being prevented - attend the meetings of the Council. A member who is unable to attend shall inform his alternate member without delay.

(6) Members of the Data Protection Commission [*Datenschutzkommission*] who are not members of the Data Protection Council shall have the right to attend meetings of the Council or its working groups. They shall have no right to vote.

(7) The deliberations of the Data Protection Council shall be confidential as long as the Council itself does not decide otherwise.

(8) The members of the Data Protection Council, the members of the Data Protection Commission and experts brought into the meeting according to para. 2 shall be obliged to keep all information confidential of which they have learned solely due to their activities for the Data Protection Council, insofar as secrecy is required in the public interest or in the interest of a party.

## **8. Abschnitt - Besondere Verwendungszwecke von Daten**

### **Private Zwecke**

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

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

### **Part 8 - Special Purposes of Data Use**

#### **Private Purposes**

**Sect. 45** (1) Natural persons shall be permitted to process data for purely personal or family matters that have been disclosed to them by the data subject [*Betroffener*] himself or that they have received in a lawful manner, in particular in accordance with sect. 7 para. 2.

(2) Data that are processed by a natural person for purely personal or family matters shall be transmitted for another purpose only with the consent of the data subject, unless expressly provided for otherwise by law.

#### **Wissenschaftliche Forschung und Statistik**

**§ 46.** (1) Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die

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

Andere Daten dürfen nur unter den Voraussetzungen des Abs. 2 Z 1 bis 3 verwendet werden.

(2) Bei Datenanwendungen für Zwecke wissenschaftlicher Forschung und Statistik, die nicht unter Abs. 1 fallen, dürfen Daten, die nicht öffentlich zugänglich sind, nur

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

verwendet werden.

(3) Eine Genehmigung der Datenschutzkommission für die Verwendung von Daten für Zwecke der wissenschaftlichen Forschung oder Statistik ist zu erteilen, wenn

1. die Einholung der Zustimmung der Betroffenen mangels ihrer Erreichbarkeit unmöglich ist oder sonst einen unverhältnismäßigen Aufwand bedeutet und
2. ein öffentliches Interesse an der beantragten Verwendung besteht und
3. die fachliche Eignung des Antragstellers glaubhaft gemacht wird.

Sollen sensible Daten übermittelt werden, muß ein wichtiges öffentliches Interesse an der Untersuchung vorliegen; weiters muß gewährleistet sein, daß die Daten beim Empfänger nur von Personen verwendet werden, die hinsichtlich des Gegenstandes der Untersuchung einer gesetzlichen Verschwiegenheitspflicht unterliegen oder deren diesbezügliche Verlässlichkeit sonst glaubhaft ist. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von

Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten, notwendig ist.

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

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

### **Scientific Research and Statistics**

**Sect. 46** (1) For the purpose of scientific or statistical research projects whose goal is not to obtain results in a form relating to specific data subjects [*Betroffene*], the controller [*Auftraggeber*] shall have the right to use all data that

1. are publicly accessible or
2. the controller has lawfully collected for other research projects or other purposes or
3. are only indirectly personal for the controller.

Other data shall only be used under the conditions specified in para. 2 sub-paras. 1 to 3.

(2) In case of the use of data [*Datenverwendung*] for purposes of scientific research or statistics that do not fall under para. 1, data which are not publicly accessible shall be used only

1. pursuant to specific legal provisions or
2. with the consent of the data subject [*Betroffener*] or
3. with a permit of the Data Protection Commission [*Datenschutzkommission*] pursuant to para. 3.

(3) A permit of the Data Protection Commission for the use of data for purposes of scientific research or statistics shall be granted if

1. the consent of the data subjects is impossible to obtain because they cannot be reached or the effort would otherwise be unreasonable and
2. there is a public interest in the use of data for which a permit is sought and
3. the professional aptitude of the applicant has satisfactorily been demonstrated.

In case sensitive data are to be transmitted, an important public interest in the research must exist; furthermore, it must be ensured that at the recipient the data shall only be used by persons who are subject to a statutory duty to confidentiality or whose reliability in this respect is otherwise credible. The Data Protection Commission may issue its permit subject to terms and conditions insofar as this is necessary to safeguard the data subjects' interests deserving protection, in particular, with regard to the use of sensitive data.

(4) Legal restrictions on the right to make use of data [*Datenverwendung*] for other reasons, in particular copyright, shall not be affected.

(5) Even in those cases where the use of data in a form which permits identification of data subjects is legal for purposes of scientific research or statistics, the data shall be coded without delay so that the data subjects are no longer identifiable if specific phases of scientific or statistic work can be performed with indirectly personal data only. Unless expressly laid down otherwise, data in a form which permits identification of data subjects shall be rendered unidentifiable as soon as it is no longer necessary for scientific or statistic work to keep them identifiable.

## Zurverfügungstellung von Adressen zur Benachrichtigung und Befragung von Betroffenen

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

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

1. Daten desselben Auftraggebers verwendet werden oder
2. bei einer beabsichtigten Übermittlung der Adreßdaten an Dritte
  - a) an der Benachrichtigung oder Befragung auch ein öffentliches Interesse besteht oder
  - b) der Betroffene nach entsprechender Information über Anlaß und Inhalt der Übermittlung innerhalb angemessener Frist keinen Widerspruch gegen die Übermittlung erhoben hat.

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

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

(4) Die Datenschutzkommission hat die Genehmigung zur Übermittlung zu erteilen, wenn der Antragsteller das Vorliegen der in Abs. 3 genannten Voraussetzungen glaubhaft macht und überwiegende schutzwürdige Geheimhaltungsinteressen der Betroffenen der Übermittlung nicht entgegenstehen. Die Datenschutzkommission kann die Genehmigung an die Erfüllung von Bedingungen und Auflagen knüpfen, soweit dies zur Wahrung der schutzwürdigen Interessen der Betroffenen, insbesondere bei der Verwendung sensibler Daten als Auswahlkriterium, notwendig ist.

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

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

## Transmission of Addresses to Inform or Interview Data Subjects

**Sect. 47** (1) Unless provided for otherwise by law, the transmission [*Übermittlung*] of address data of a certain group of data subjects [*Betroffene*] in order to inform or interview them shall require the consent of the data subjects.

(2) If an infringement of the data subject's interests in secrecy is unlikely, considering the selection criteria for the category of data subjects [*Betroffenenkreis*] and the subject of the information or interviews, no consent shall be required if

1. data from the same controller are used or

2. in case of an intended transmission of address data to third parties
  - a) there is an additional public interest in the information or interviewing or
  - b) the data subject, having received an adequate information about the cause for and content of the transmission, has not objected to the transmission within a reasonable period of time.

(3) If the prerequisites of para. 2 are not met and if obtaining the consent of the data subjects' pursuant to para. 1 would require an unreasonable effort, the transmission of the address data shall be permissible with a permit of the Data Protection Commission [*Datenschutzkommission*] pursuant to para. 4, in case the transmission to third parties shall be performed for

1. the purpose of information or an interview due to an important interest of the data subject himself
2. an important public interest in the information or interviews or
3. an interview of the data subjects for reasons of scientific research and statistics.

(4) The Data Protection Commission shall grant the permit for the transmission if the controller has satisfactorily demonstrated that one of the requirements in para. 3 applies and no overriding interests in secrecy deserving protection on the part of the data subject are an obstacle to the transmission. The Data Protection Commission may issue the permit subject to terms and conditions, insofar as this is necessary to safeguard the data subjects' interests deserving protection, in particular, with regard to the use of sensitive data as selection criterion.

(5) The transmitted address data shall only be used for the permitted purpose and shall be erased as soon as they are no longer needed for information or interviews.

(6) In those cases where it is lawful to transmit the names and addresses of persons belonging to a certain category of data subjects pursuant to the aforementioned provisions, the processing required for selecting the address data to be transmitted shall also be permitted.

### **Publizistische Tätigkeit**

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

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

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

### **Journalistic Purposes**

**Sect. 48** (1) Insofar as media companies, media services and their operatives use data directly for journalistic purposes according to the Media Act [*Mediengesetz*<sup>35</sup>], only sects. 4 to 6, 10, 11, 14 and 15 of the non-constitutional provisions of this Federal Act [*Bundesgesetz*] shall apply.

(2) The use of data [*Datenverwendung*] for activities pursuant to para. 1 shall be legal insofar as this is required to fulfil the information requirements of the media companies, media services and their operatives in exercise of the right to free speech pursuant to art. 10 para. 1 of the European Convention on Human Rights.

---

<sup>35</sup> *Mediengesetz* (Media Act), Federal Law Gazette No. 314/1981

(3) In all other respects the Media Act [*Mediengesetz*] shall apply, especially the third part about the protection of personality rights.

## **9. Abschnitt - Besondere Verwendungsarten von Daten**

### **Automatisierte Einzelentscheidungen**

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

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

1. dies gesetzlich ausdrücklich vorgesehen ist oder
2. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertrages ergeht und dem Ersuchen des Betroffenen auf Abschluß oder Erfüllung des Vertrages stattgegeben wurde oder
3. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen - beispielsweise die Möglichkeit, seinen Standpunkt geltend zu machen - garantiert wird.

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

### **Part 9 - Special Uses of Data**

#### **Automated Individual Decisions**

Sect. 49 (1) Nobody shall be subjected to a decision that produces legal effects concerning him or adversely affects him in a significant manner which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, for example his performance at work, creditworthiness, reliability and conduct.

(2) Deviating from para. 1, a person may be subjected to a decision based solely on automated processing if

1. this is expressly authorised by law or
2. the decision is taken in the course of the entering into or performance of a contract, and the request of the data subject [*Betroffener*] for the entering into or the performance of the contract has been satisfied or
3. the legitimate interests of the data subject are safeguarded by appropriate means - such as arrangements allowing him to assert his point of view.

(3) Upon request, the data subject shall in case of automated decisions be informed of the logical procedure of the automated decision in an intelligible form.

#### **Informationsverbundsysteme**

**§ 50.** (1) Die Auftraggeber eines Informationsverbundsystems haben, soweit dies nicht bereits durch Gesetz geregelt ist, einen geeigneten Betreiber für das System zu bestellen. Name (Bezeichnung) und Anschrift des Betreibers sind in der Meldung zwecks Eintragung in das Datenverarbeitungsregister bekannt zu geben. Unbeschadet des Rechtes des Betroffenen auf Auskunft nach § 26 hat der Betreiber jedem Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen; in Fällen, in welchen der Auftraggeber gemäß § 26 Abs. 5 vorzugehen hätte, hat der Betreiber mitzuteilen, daß kein der Pflicht zur Auskunftserteilung unterliegender Auftraggeber benannt werden kann. Die Unter-



stützungspflicht des Betreibers gilt auch bei Anfragen von Behörden. Den Betreiber trifft überdies die Verantwortung für die notwendigen Maßnahmen der Datensicherheit (§ 14) im Informationsverbundsystem. Von der Haftung für diese Verantwortung kann sich der Betreiber unter den gleichen Voraussetzungen, wie sie in § 33 Abs. 3 vorgesehen sind, befreien. Wird ein Informationsverbundsystem geführt, ohne daß eine entsprechende Meldung an die Datenschutzkommission unter Angabe eines Betreibers erfolgt ist, treffen jeden einzelnen Auftraggeber die Pflichten des Betreibers.

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

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

### **Joint Information Systems**

**Sect. 50** (1) The controllers [*Auftraggeber*] of a joint information system [*Informationsverbundsystem*] shall, unless already regulated by law, appoint a suitable operator [*Betreiber*] for the system. The name (designation) and address of the operator shall be included in the notification for registration in the Data Processing Register [*Datenverarbeitungsregister*]. Without prejudice to the data subject's rights pursuant to sect. 26, the operator shall give to the data subject [*Betroffener*] upon request within twelve weeks all information necessary to identify the controller who is responsible for the data processed in the system concerning him; in cases where the controller would have to apply sect. 26 para. 5, the operator shall inform the data subject that no controller obligated to give the information can be named. The operator's obligation to assist shall also apply in case of requests by public authorities. The operator shall also be responsible for the necessary data security measures (sect. 14) in the joint information system. The operator can free himself of liability under the conditions laid down in sect. 33 para. 3. If a joint information system is operated and no appropriate notification with an appointed operator is filed with the Data Processing Register, each controller shall have to bear the obligations of the Operator.

(2) Further controller duties may be assigned to the operator by an appropriate legal instrument. Unless realised by statute, such assignment of obligations shall only be valid vis-à-vis the data subject and the public authorities that execute this Federal Act [*Bundesgesetz*] if the assignment is recorded in the Data Processing Register [*Datenverarbeitungsregister*] following an appropriate notification to the Data Protection Commission [*Datenschutzkommission*].

(3) The provisions of para. 1 and 2 shall not apply if provided for otherwise by law due to the special, in particular, international structure of a specific joint information system.

## **10. Abschnitt - Strafbestimmungen**

### **Datenverwendung in Gewinn- oder Schädigungsabsicht**

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

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

## **Part 10 - Penal Provisions**

### **Use of Data with the Intention to make a Profit or to Cause Harm**

**Sect. 51** (1) Whoever uses personal data that have been entrusted to or made accessible to him solely because of professional reasons, or that he has acquired illegally, for himself or makes such data available to others or publishes such data with the intention to make a profit or to harm others, despite the data subject's interest in secrecy deserving protection, shall be punished by a court with imprisonment up to a year, unless the offence shall be subject to a more severe punishment pursuant to another provision.

(2) The offender shall be prosecuted only with the authorisation of the injured party.

### **Verwaltungsstrafbestimmung**

**§ 52.** (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 18 890 Euro zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder
4. Daten vorsätzlich entgegen § 26 Abs. 7 löscht.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 9 445 Euro zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 17 erfüllt zu haben oder
2. Daten ins Ausland übermittelt oder überläßt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben oder
3. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24 oder 25 verletzt oder
4. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht läßt.

(3) Der Versuch ist strafbar.

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

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

## Administrative Penalties

**Sect. 52** (1) Insofar as the act does not realise the legal elements of a criminal offence subject to the jurisdiction of the courts of law and is not subject to more severe penalties according to another administrative provision, an administrative offence punishable by a fine of up to 18 890 Euro is committed by anyone who

1. intentionally and illegally gains access to a data application [*Datenanwendung*] or maintains an obviously illegal means of access or
2. transmits data intentionally in violation of the rules on confidentiality (sect. 15), and in particular anybody who uses data entrusted to him according to sect. 46 and 47 for other purposes or
3. uses or fails to grant information, to rectify or erase data in violation of a final judicial decision or ruling [*Bescheid*],
4. intentionally erases data in violation of sect. 26 para. 7.

(2) Insofar as the act does not realise the legal elements of a criminal offence subject to the jurisdiction of the courts of law, an administrative offence punishable by a fine of up to 9 445 Euro is committed by anyone who

1. collects, processes and transmits data without having fulfilled his obligation to notify according to sect. 17 or
2. engages in transborder data transmissions [*Übermittlungen*] or commitments [*Überlassungen*] without the necessary permit of the Data Protection Commission [*Datenschutzkommission*] according to sect. 13 or
3. violates his obligations of disclosure and information according to sects. 23, 14 and 25 or
4. grossly neglects the required data security measures according to sect. 14.

(3) Attempts shall be punished<sup>36</sup>.

(4) Data media or programs can be confiscated (sects. 10, 17 and 18 VStG<sup>37</sup>), if they are linked to an administrative offence according to para. 1 and 2.

(5) The District Administrative Authority [*Bezirksverwaltungsbehörde*] at the controllers [*Auftraggeber*] (processors [*Dienstleister*]) domicile or seat shall be the competent authority for decisions according to para. 1 to 4. If there is no domicile or seat in Austria, the District Administrative Authority at the seat of the Data Protection Commission [*Datenschutzkommission*] shall be competent.

---

<sup>36</sup> This is a peculiarity of Austrian administrative law. According to sect. 8 para. 1 *Verwaltungsstrafgesetz 1991* (Administrative Penal Code 1991), Federal Law Gazette No. 52/1991, an attempt to commit an act that is punishable with administrative sanctions shall be punished only if specifically provided by law.

<sup>37</sup> Vstg: *Verwaltungsstrafgesetz 1991* (Administrative Penal Code 1991), Federal Law Gazette No. 52/1991.

## **11. Abschnitt - Übergangs- und Schlußbestimmungen**

### **Befreiung von Gebühren, Abgaben und vom Kostenersatz**

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

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

## **Part 11 - Transitional and Final Provisions**

### **Exemption from Fees**

**Sect. 53** (1) All applications submitted according to this Federal Act [*Bundesgesetz*] by data subjects [*Betroffener*] to safeguard their interests as well as all applications in the proceedings for notification and for register statements according to sect. 21 para. 3 shall be exempt from stamp duties and federal administrative fees.

(2) No fee shall be charged for copies of entries in the Data Processing Register [*Datenverarbeitungsregister*] needed by a data subject to assert his rights.

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

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

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

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

### **Communication to the European Commission and to the other Member States of the European Union**

**Sect. 54** (1) The Federal Chancellor [*Bundeskanzler*] shall communicate to the European Commission whenever a Federal Act [*Bundesgesetz*] concerning the right to process sensitive data has been adopted upon its promulgation in the Federal Law Gazette [*Bundesgesetzblatt*].

(2) The Data Protection Commission [*Datenschutzkommission*] shall communicate to the other member states of the European Union and the European Commission in which cases

1. no permit was issued for transborder data flows to a third country because the requirements of sect. 13 para. 2 sub-para 1 were considered not to have been met;
2. a permit was issued for transborder data flows to a third country without an adequate level of data protection because the requirements of sect. 13 para. 2 sub-para 2 are deemed to have been met.

## Feststellungen der Europäischen Kommission

**§ 55.** Der Inhalt der in einem Verfahren gemäß Art. 31 Abs. 2 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. Nr. L 281 vom 23. November 1995, S. 31, getroffenen Feststellungen der Europäischen Kommission über

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

ist vom Bundeskanzler im Bundesgesetzblatt gemäß § 2 Abs. 3 BGBIG, BGBl. Nr. 660/1996, kundzumachen.

## Measures of the European Commission

**Sect. 55** The content of findings of the European Commission made according to Art. 31 para. 2 of the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23 November 1995 p. 0031, on

1. whether a third country has an adequate level of data protection or
2. the suitability of certain standard contractual clauses or pledges to safeguard sufficient protection to the use of data [*Datenverwendung*] in a third country

shall be promulgated by the Federal Chancellor [*Bundeskanzler*] in the Federal Law Gazette according to sect. 2 para. 3 BGBIG<sup>38</sup>, Federal Law Gazette No. 660/1996.

## Verwaltungsangelegenheiten gemäß Art. 30 B-VG

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

## Administrative Matters pursuant to Art. 30 of the Federal Constitution

**Sect. 56** The President of the National Council [*Nationalrat*] is the controller [*Auftraggeber*] of such data applications [*Datenanwendungen*] for purposes of such matters with which he has been entrusted pursuant to art. 30 B-VG<sup>39</sup>. Transmissions of data [*Übermittlungen*] from such data applications shall only take place if ordered by the President of the National Council. The President shall make provisions that in case of a transmission order the requirements of sect. 7 para. 2 are met and, in particular, that the consent of the data subject [*Betroffener*] is obtained in such cases where it is necessary pursuant to sect. 7 para. 2 for lack of another legal basis for the transmission.

## Sprachliche Gleichbehandlung

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

---

<sup>38</sup> BGBIG: *Bundesgesetzblattgesetz* (Law on the Federal Law Gazette), Federal Law Gazette No. 660/1996.

<sup>39</sup> B-VG: *Bundes-Verfassungsgesetz* (Federal Constitutional Act), Federal Law Gazette No. 1/1930.

## Gender-Neutral Use of Language

**Sect. 57** Insofar as expressions relating to natural persons in this article are given only in the male form, they shall apply to males and females equally. When the expressions are applied to specific natural persons, the form specific to the gender shall be used.

## Manuelle Dateien

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

## Manual Filing Systems

**Sect. 58** Insofar as manual filing systems, i.e., filing systems [*Dateien*] managed without automatic processing, exist for such purposes and fields where the Federation [*Bund*] has the power to pass laws, they are deemed to be data applications [*Datenanwendungen*] according to sect. 4 sub-para. 7. Sect. 17 shall apply insofar as the obligation to notification applies only to those filing systems whose content is subject to prior checking [*Vorabkontrolle*] according to sect. 18 para. 2.

## Umsetzungshinweis

**§ 59.** Mit diesem Bundesgesetz wird die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995, S 31, umgesetzt<sup>40</sup>.

## Implementation Notice

**Sect. 59** This Federal Act [*Bundesgesetz*] implements the Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23 November 1995 p. 31<sup>41</sup>.

## Inkrafttreten

**§ 60. (1) (Verfassungsbestimmung)** Die Verfassungsbestimmungen des Art. 1, der §§ 35 Abs. 2, 37, 38 Abs. 1 und 61 Abs. 4 und 7 treten mit 1. Jänner 2000 in Kraft. Mit dem Inkrafttreten dieses Bundesgesetzes tritt das Datenschutzgesetz, BGBl. Nr. 565/1978 in der geltenden Fassung, außer Kraft.

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

(3) §§ 26 Abs. 6 und 52 Abs. 1 und 2 in der Fassung des Bundesgesetzes BGBl. I Nr. 136/2001 treten mit 1. Jänner 2002 in Kraft.

## Entry into Force

**Sect. 60 (1) (Constitutional Provision)** The constitutional provisions of art. 1, sects. 35 para. 2, 37, 38 para. 1 as well as 61 para. 4 and 7 shall enter into force on 1 January 2000. With the entry into force of this Federal Act [*Bundesgesetz*] the Datenschutzgesetz, Federal Law Gazette No. 565/1978, shall become ineffective.

---

<sup>40</sup> Diese Richtlinie ist im Internet auf der Website der Datenschutzkommission veröffentlicht.

<sup>41</sup> The Directive can be downloaded in English from the website of the data protection commission.

(2) The other provisions of this Federal Act shall enter into force on 1 January 2000 as well.

(3) Sects. 26 para. 6 and 52 para. 1 and 2 as formulated in the federal law published in Federal Law Gazette I No. 136/2001 shall enter into force on 1 January 2002.

## Übergangsbestimmungen

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

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

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

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

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

(6) Die zum Zeitpunkt des Inkrafttretens dieses Gesetzes im Amt befindliche Datenschutzkommission übernimmt für den Zeitraum von sechs Monaten ab Inkrafttreten dieses Gesetzes die Funktion der Datenschutzkommission gemäß § 35.

(7) **(Verfassungsbestimmung)** Soweit in einzelnen Vorschriften Verweise auf das Datenschutzgesetz, BGBl. Nr. 565/1978, enthalten sind, gelten diese bis zu ihrer Anpassung an dieses Bundesgesetz sinngemäß weiter.

## Transitional Provisions

**Sect. 61** (1) Notifications that were made to the Data Processing Register [*Datenverarbeitungsregister*] before this Federal Act [*Bundesgesetz*] entered into force shall count as notifications according to sect. 17, insofar as they have not become irrelevant because the obligation to notify is no longer applicable. Likewise, registrations made before this Federal Act entered into force shall count as registrations according to sect. 21.

(2) Insofar as the law as it now stands requires a permit for transborder data transmission [*Übermittlung*], an application for a new permit must be filed before 1 January 2003 for such transmissions for which a permit was granted prior to this Federal Act's entry into force. If the application is filed in time, such transmissions may be carried out until the final decision about the application for the permit.

(3) Data protection violations that have taken place before this Federal Act entered into force shall, insofar as the legality or illegality of a set of facts is concerned, be adjudicated according to the legal provisions in force at the time the act was committed; insofar as an obligation to act or a forbearance is concerned, the law as it stands at the time when the decision of first instance is rendered shall be applied. A criminal offence shall be adjudicated according to the law that is more favourable to the offender overall; this also extends to appeal proceedings.

(4) **(Constitutional Provision)** Data applications [*Datenanwendungen*] that are required for the purposes laid down in sect. 17 para. 3 may be continued even without a sufficient legal basis in terms of sect. 1 para. 2 until 31 December 2007, in the cases of sect. 17 para. 3 sub-para. 1 to 3 until federal regulations covering the functions and powers in these fields are enacted.

(5) Manual filing systems subject to notification according to sect. 58 shall be notified to the Data Processing Register no later than 1 January 2003, provided they already existed when this Federal Act entered into force. The same shall apply to automated data applications according to sect. 17 para. 3 that were made subject to notification by the new regulations.

(6) The Data Protection Commission [*Datenschutzkommission*] in office at the time this Federal Act enters into force shall carry out all functions of the Data Protection Commission according to sect. 35 for six months after this Federal Act has entered into force.

(7) **(Constitutional Provision)** Insofar as individual provisions contain references to the Data Protection Act [*Datenschutzgesetz*], Federal Law Gazette No. 565/1978, such provisions shall be valid by analogous application until adjusted to conform to this Federal Act.

## Verordnungserlassung

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

## Enactment of Ordinances

**Sect. 62** Ordinances [*Verordnungen*] based on this Federal Act [*Bundesgesetz*] in the current version in force may already be enacted as of the day following the promulgation of the legal provision to be implemented; they shall, however, not enter into force before the statutory provisions which are to be implemented.

## Verweisungen

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

## References

**Sect. 63** Insofar as provisions of this Federal Act [*Bundesgesetz*] refer to provisions of other Federal Acts, these shall be applied in the current version in force<sup>42</sup>.

---

<sup>42</sup> Federal Acts are normally quoted with the title and the Federal Law Gazette number of the first publication. This provision states that an act that has been amended several times shall be applied in the up-to-date version.



## **Vollziehung**

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

## **Execution**

**Sect. 64** The Federal Chancellor [*Bundeskanzler*] and the other Federal Ministers [*Bundesminister*] within their purview shall execute this Federal Act [*Bundesgesetz*] insofar as the execution has not been entrusted to the Federal Government [*Bundesregierung*] or to the State Governments [*Landesregierungen*].