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. The laws full name and source should be given as "Datenschutzgesetz 2000 (DSG 2000), Austrian Federal Law Gazette part I No. 165/1999".

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.)

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.

This text contains only the English translation to reduce the size of the file. Professional

users are advised to download the German version as well, or to use the PDF or RTF versions, which contain both the German and the English text.

Please note that this law may be amended in the future, and check occasionally for updates.

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 [1] 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, 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; 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 [2] .

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

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 form paras. 1 to 3 shall be permissible only in matters not subject to the jurisdiction of the European Union.

Article 2 ➦

Part 1 - General Provisions ➦

Definitions

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

"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;

"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;

"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);

"Controller" ["Auftraggeber"]: natural or legal person, group of persons or organ of a territorial corporate body [Gebietskörperschaft] [3] or the offices [4] 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;

"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);

"Filing System" [5] ["Datei"]:structured set of personal data which are accessible according to at least one specific criterion;

"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);

"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);

"Processing of Data" ["Verarbeiten von Daten"]: the collection, recording, storing, sorting, comparing, modification, interlinkeage, 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);

"Collection of Data" ["Ermitteln von Daten"]: The acquisition of data with the intention of using them in a data application;

"Committing of Data" ["Überlassen von Daten"]: the transfer of data from the controller to a processor;

"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;

"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;

"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;

"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.

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

   are established according to public law legal structures, in particular also as an organ of a territorial corporate body [Gebietskörperschaft], or

   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].

Part 2 - Use of Data ➦

Principles

Sect. 6.

1. Data shall only

   be used fairly and lawfully;

   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;

   be used insofar as they are essential for the purpose of the data application [Datenanwendung] and are not excessive in relation to the purpose;

   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;

   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.

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

   they originate from a legal data application according to para. 1 and

   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

   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.

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

   an explicit legal authorisation or obligation to use the data exists; or

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

vital interests of the data subject require the use; or

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

is an essential requirement for a controller of the public sector to exercise a legally assigned function or

is performed by a controller of the public sector in fulfilment of his obligation to provide inter-authority assistance [6] or

is required to protect the vital interests of a third party or

is necessary for the fulfilment of a contract between the controller and the data subject or

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

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

an explicit legal obligation or authorisation to use the data exists; or

the use of such data is an essential requirement for a controller of the public sector to exercise a legally assigned function;

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].

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

the data subject [Betroffener] has obviously made public the data himself or

the data are used only in indirectly personal form or

the obligation or authorisation to use the data is stipulated by laws, insofar as these serve an important public interest, or

the use is made by a controller of the public sector in fulfilment of his obligation to give inter-authority assistance or

data are used that concern solely the exercise of a public office by the data subject or

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

the processing or transmission [Übermittlung] is in the vital interest of the data subject and his consent cannot be obtained in time or

the use is in the vital interest of a third party or

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

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

the use is required according to the rights and duties of the controller in the field of employment law and civil service regulations [7] and, and is legitimate according to specific legal provisions; the rights of the labour councils according to the Arbeitsverfassungsgesetz [8] with regard to the use of data [Datenverwendung] remain unaffected, or

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

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.

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

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]:

   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;

   to take all required safety measures pursuant to sect. 14; in particular to employ only operatives who have committed themselves to confidentiality vis-á-vis the processor or are under a statutory obligation of confidentiality;

   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;

   - 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;

   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;

   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;

Transborder [9] 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 [10] . 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

   the data have been published legitimately in Austria or

   data are transferred or committed that are only indirectly personal to the recipient or

   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

   data from a data application [Datenanwendung] for private purposes (sect. 45) or for journalistic purposes (sect. 48) is transmitted or

   the data subject [Betroffener] has without any doubt given his consent to the transborder transmission or committing or

   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

   the transmission is necessary for the establishment, exercise or defence of legal claims before a foreign authority and the data were collected legitimately or

   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

   the data exchange is with Austrian governmental missions and offices in foreign countries or

   the transmissions or committings 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

to safeguard an important public interest or

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 committings 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 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.

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

   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

   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 [11] .

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 [12] and enter the fact that authorisation has been granted into the Data Processing Register

[Datenverarbeitungsregister] (sect. 16).

5. Deviating from para. 1, a domestic processors [Dienstleister] can apply for a permit if, in order to fulfil his contractual duties vis-á-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 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.

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:

   The distribution of functions between the organisational units as well as the operatives regarding the use of data [Datenverwendung] shall be laid down expressly,

   The use of data must be tied to valid orders of the authorised organisational units or operatives,

   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,

   The right of access to the premises of the data controller or processor is to be regulated,

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,

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,

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,

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 [13] (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.

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.

4. Without prejudice to the constitutional right to issue instructions [Weisungen] [14] , 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.

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 [15] [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.

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

   which solely contain published data or

   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

   which contain only indirectly personal data or

   which are carried out by natural persons for activities that are entirely personal or concern just the person's family life (sect. 45) or

   which are carried out for journalistic purposes according to sect. 48 or

   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 [16] .

3. Furthermore, data applications for the purpose of

   protecting the constitutional institutions of the Republic of Austria or

   safeguarding the operational readiness of the federal army or

   safeguarding the interests of comprehensive national defence or

   protecting important foreign policy, economic or financial interests of the Republic of Austria or the European Union

   preventing and prosecuting of crimes [17]

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

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

that involve sensitive data or

that involve data about offences according to sect. 8 para. 4 or

whose purpose is to give information on the data subjects [Betroffener] creditworthiness or

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.

Required Content of the Notification

Sect. 19

1. A notification pursuant to sect. 17 must contain

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

the proof of statutory competence or of the legitimate authority that the controller's activities are permitted, if so required and

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

the categories of data subjects [Betroffenenkreise] and the categories of data [Datenarten] about them that are processed and

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

- 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

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 [18] [Verordnung]. Notifications of data applications whose content corresponds to a Model Application need to contain only the following:

the designation of the model application [Musteranwendung] according to the model ordinance [Musterverordnung] and

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

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.

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 19 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.

Registration

Sect. 21

1. Notifications pursuant to sect. 19 are to be entered into the Data Processing Register [Datenverarbeitungsregister] if

   the checking procedure has shown that a registration is permitted or

   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

   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.

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.

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.

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.

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

   the purpose of the data application for which for which the data are collected, and

   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

   the data subject has a right to object to intended processing or transmission of data pursuant to sect. 28 or

   it is not clear for the data subject under the circumstances whether he is required by law to reply to the questions posed, or

   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

   if the use of data [Datenverwendung] is provided for by law or an ordinance [Verordnung] or

   if it is impossible to provide the information because the data subjects cannot be reached or

   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.

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.

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

   to protect of the constitutional institutions of the Republic of Austria or

to safeguard of the operational readiness of the federal army or

to safeguard the interests of comprehensive national defence or

to protect important foreign policy, economic or financial interests of the Republic of Austria or the European Union or

to prevent and prosecute crimes [20] .

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.

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]

   on his own, as soon the incorrectness of the data or the inadmissibility of the processing becomes know to him, or

   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

   the obligation to rectification and erasure ex officio or

   the procedure to assert and the competence to decide applications to rectification and erasure of data subjects

   is not regulated otherwise by federal law.

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 he 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.

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.

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 [21] regarding such crimes [22] 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,

   initiate an administrative inquiry to check the registration pursuant to sect. 22 para. 4., or

   bring a criminal charge pursuant to sects. 51 or 52, or

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

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 my 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.

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-á-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.

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 [23] 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 [24]) [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).

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 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 [25] shall apply.

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

according to Sect. 32 para. 4.

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 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.

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-á-vis the highest executive authorities enumerated in art. 19 B-VG [26] .

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

   a proposal of three candidates by the President of the Supreme Court [27] [Oberster Gerichtshof] for the judge,

   a proposal of the states [Bundesländer] for two members,

   a proposal of three candidates by the Federal Chamber of Labour [28] [Bundeskammer für Arbeiter und Angestellte] for one member,

   a proposal of three candidates by the Austrian Federal Economic Chamber [29] [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.

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:

   members of the Federal Government [Bundesregierung] or of a State Government [Landesregierung] or Secretaries of State [Staatssekretäre];

   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 [30] of the Federal Government upon request of the Federal Chancellor.

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.

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 [31] [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.

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.

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 [32] [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 [33] [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.

Establishment and Duties of the Data Protection Council

Sect. 41

1. A Data Protection Council [Datenschutzrat] is [34] 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,

the Data Protection Council can deliberate on questions of fundamental importance for data protection;

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;

public sector controllers shall present their projects to the Data Protection Council for evaluation, insofar as these are significant for data protection;

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;

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;

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.

Composition of the Data Protection Council

Sect. 42

1. The Data Protection Council [Datenschutzrat] shall have the following members:

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;

one representative each from Federal Chamber of Labour [Bundeskammer für Arbeiter und Angestellte] and the Austrian Federal Economic Chamber [Wirtschaftskammer Österreich];

two representatives of the States [Länder];

one representative each of the Association of Austrian Municipalities [Gemeindebund] and the Austrian Association of Towns [Städtebund];

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.

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.

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.

Part 8 - Special Purposes of Data ➦

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.

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

   are publicly accessible or

the controller has lawfully collected for other research projects or other purposes or

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. /P>

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

pursuant to specific legal provisions or

with the consent of the data subject [Betroffener] or

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

the consent of the data subjects is impossible to obtain because they cannot be reached or the effort would otherwise be unreasonable and

there is a public interest in the use of data for which a permit is sought and

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.

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

   data from the same controller are used or

   in case of an intended transmission of address data to third parties

   there is an additional public interest in the information or interviewing or

   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

   the purpose of information or an interview due to an important interest of the data subject himself

   an important public interest in the information or interviews or

   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 s 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.

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] [35] , 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.

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

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

   this is expressly authorised by law or

   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

   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.

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.

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.

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

   intentionally and illegally gains access to a data application [Datenanwendung] or maintains an obviously illegal means of access or

   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

   uses or fails to grant information, to rectify or erase data in violation of a final judicial decision or ruling [Bescheid],

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

   collects, processes and transmits data without having fulfilled his obligation to notify according to sect. 17 or

   engages in transborder data transmissions [Übermittlungen] or committings [Überlassungen] without the necessary permit of the Data Protection Commission [Datenschutzkommission] according to sect. 13 or

   violates his obligations of disclosure and information according to sects. 23, 14 and 25 or

   grossly neglects the required data security measures according to sect. 14.

3. Attempts shall be punished [36] .

4. Data media or programs can be confiscated (sects. 10, 17 and 18 VStG [37]), 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.

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.

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

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;

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.

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

whether a third country has an adequate level of data protection or

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 BGBlG [38] , Federal Law Gazette No. 660/1996.

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 [39] . 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.

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.

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.

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 [40] .

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.
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.

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 Acts 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 its 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.

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.

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 [41] .

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].

1:

The term law is to be understood in the sense of "statute" according to the continental European legal tradition.

➦

2:

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 administrating their personnel.

➦

3:

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].

4:

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.

5:

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.

6:

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).

7:

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).

8:

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

9:

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".

10:

Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV), Federal Law Gazette II Nr. 521/1999.

11:

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

12:

Here, the word "file" means a collection of documents belonging to a specific case.

13:

StGB: Strafgesetzbuch (Penal Code), Federal Law Gazette No. 60/1974.

14:

This refers to the right of superiors in administrative authorities to issue instructions.

15:

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

16:

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

17:

The two German nouns "Vorbeugung" and "Verhinderung" both mean prevention in English.

18:

See footnote 16.

19:

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).

20:

See footnote 17.

21:

StPO: Strafprozeßordnung 1975 (Code of Criminal Procedure), Federal Law Gazette No. 631/1975.

22:

The German words "Verbrechen und Vergehen" refers to a distinction between lesser (Vergehen) and more severe crimes (Verbrechen).

23:

EO: Exekutionsordnung (Enforcement Proceedings Act), Federal Law Gazette No. 79/1896.

24:

ZPO: Zivilprozessordnung (Code of Civil Procedure), Imperial Law Gazette No. 113/1895

25:

ABGB: Allgemeines bürgerliches Gesetzbuch (Austrian General Civil Code), JGS No. 946/1811

26:

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.

27:

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.

28:

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

29:

http://www.wk.or.at/

30:

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

31:

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.

32:

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.

33:

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

34:

The Data Protection Council is already established; therefore, the wording merely confirms its existence.

35:

Mediengesetz (Media Act), Federal Law Gazette No. 314/1981

36:

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.

37:

Vstg: Verwaltungsstrafgesetz 1991 (Administrative Penal Code 1991), Federal Law Gazette No. 52/1991.

38:

BGBlG: Bundesgesetzblattgesetz (Law on the Federal Law Gazette), Federal Law Gazette No. 660/1996.

39:

B-VG: Bundes-Verfassungsgesetz (Federal Constitutional Act), Federal Law Gazette No. 1/1930.

40:

The Directive can be downloaded in English from http://www.bka.gv.at/datenschutz/eulaw.htm

41:

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.