Bundesgesetz vom 18. Oktober 1978
über den Schutz personenbezogener Daten
(Datenschutzgesetz - DSG)

Federal Act from the 18. of October 1978
on the protection of personal data
(Data Protection Act - DSG)

Federal Law Gazette (Bundesgesetzblatt) No. 565/1978,

amended No. 314/1981,
No. 577/1982 (errata correction),
No. 370/1986,
No. 605/1987,
No. 233/1988,
No. 609/1989,
No. 91/1993,
No. 79/1994,
No. 632/1994.

(**This translation is unofficial.**
The Austrian Federal Government will not assume
any responsibility for misunderstandings arising from this translation.)

ARTICLE 1

(Constitutional Provision)

Fundamental Right to Data Protection

Sec. 1. (1) Everyone shall have the right that his personal data are kept secret insofar as he has an interest in such data that needs protection, in particular as regards the respect of his privacy and family life.

(2) Any limitations of the right granted in p. 1 shall be permitted only for the safeguarding of justified interest of a third party or on the basis of laws necessary for the reasons stated in Art. 8, p. 2 of the European Convention on Human Rights (Federal Law Gazette No. 210/1958). Even in the case of such limitations priority shall be given to the confidentiality of the personal data.

(3) Everyone shall, within the limits of legal provisions, have the right to information as to who is collecting or processing his personal data, their sources, their nature and content and their utilisation, insofar as his data are subject to automated processing.

(4) Everyone shall, within the limits of legal provisions, have the right to rectification of incorrect data and to deletion of illegally collected or processed data, insofar, as his data are subject to automated processing.

(5) Limitations of the rights stated in p. 3 and 4 shall be permitted only under the conditions stated in p. 2.

(6) Insofar as persons or entities act under private law, the fundamental right to data protection shall be asserted by recourse to the ordinary courts.

Legislative Competence and Enforcement

Sec. 2. (1) The Federation shall have the legislation on the protection of personal data in automated data traffic.

(2) The Federation shall have power to execute such Federal laws. Insofar as such data are collected, processed or communicated by a Land, on behalf of a Land, by or on behalf of legal persons established by law within the competence of the Länder these Federal laws shall be executed by the States unless the execution has been entrusted by Federal law to the Data Protection Commission, the Data Protection Council or the courts.

ARTICLE 2
PART 1
General Provisions

Sec. 3. For the following provisions of the Act the terms listed below are defined as follows:

1. **Data:** information stored on a data medium concerning an identified or with great probability identifiable subject (*personal data*);

2. **Data Subject:** any natural or legal person or association different from the data controller (p. 3), whose data are applied (p. 12); legal persons of public law and their organs shall not be considered to be data subjects insofar as they exercise official functions;

3. **Data Controller:** any person, organisation or organ of a legal person of public law, who processes or by consulting a service processor (p. 4) obtains data processed by automated means;

4. **Service Processor:** any person, organisation or organ of a legal person of public law, who uses data on the basis of such a mandate of a data controller, which especially aims at automated processing of data;

5. **EDP (Electronic Data Processing):** the course of steps of processing (p. 7), which are organised in order to reach a defined result (purpose) and which - as a whole or partly - are performed automated (i.e. using machines and controlled by programs), if personal data can be selected out of all data stored according to at least one characteristic on the basis of the machinery and programs actually used;

6. **Collection of Data:** the gathering or other acquisition of data for EDP;

7. **Processing of Data:** the recording, storing, sorting, comparing, modification, interlinkeage, reproduction, communication or deletion of data within EDP;

8. **Use of Data:** any kind of handling of data performed by a data controller or a data processor, which is not collection, processing or transmission;

9. **Transmission of Data:** the transfer of processed data to a recipient other than the data subject, the data controller or the data processor, in particular the publication of such data as well as their use for other purposes;

10. **Committing of Data:** the transfer of data from a data controller to a data processor or from one data processor to another;

11. **Deletion of Data:**
a) the obliteration of data in such a way that no reconstruction is possible *(physical deletion)*;
b) the blocking of access to data by adequate means of programming *(logical deletion)*;

12. **Data Traffic (Application of data)**: collection, processing, use, transmission and committing of data or one of these operations.

Sec. 4. (1) The provisions of Part 2 shall apply to data traffic of or on behalf of legal subjects established by law other than legal subjects under Sec. 5. below.

(2) By order of the Federal Government legal subjects as defined in p. 1 shall - after consultation with the Data Protection Council, to the extent they exercise their activities under private law, be exempted in respect of these activities from the application of Part 2. For such legal subjects Part 3 shall apply. Such orders shall be subject to the approval of the Main Committee of the National Assembly.

(3) Secs. 8., 9., 11. and 12. shall not apply to the processing of data insofar as such processing is necessary:

1. for the protection of constitutional institutions of the Republic of Austria as well as for purposes of the administration of penal law, or

2. for the safeguarding of the military preparedness of the Federal Army, or

3. for comprehensive national defence.

This exemption shall be subject to an order of the Federal Government after consultation of the Data Protection Council and in agreement with the Main Committee of the National Assembly. The order shall lay down in detail all exemptions such as the kind of data, processing elements, etc.

Sec. 5. (1) The provisions of Part 2 shall apply to the processing of data by or on behalf of the Länder, by or on behalf of legal persons established by law within the competence of the Länder as well as by or on behalf of Gemeinden or associations of them, subject to the provision that the data protection order (Sec. 9.) as well as the amount of cost compensation for information (Sec. 11 p. 4) shall be laid down by the Land Government.

(2) Legal subjects under p. 1 above shall, to the extent they exercise their activities under private law, be exempted in respect of these activities from the application of Part 2 by means of a Land Government order to be issued after consultation of the Data Protection Council. For such areas Part 3 shall apply.

PART 2
Public sector

Permissibility of collection and processing

Sec. 6. Data may be collected and processed for purposes of automated data processing only if such is expressly authorised by law, or an essential prerequisite to enable the data controller to fulfil the tasks entrusted to him by law.

Permissibility of transmission

Sec. 7. (1) Processed data may be transmitted only if

1. such is expressly authorised by law, or

2. the data subject has expressly and in writing agreed to the transmission, which consent may be revoked in writing, or

3. data are transmitted exclusively for statistical purposes to the Austrian Central Office of Statistics and are rendered anonymous there.

(2) Transmission of data to organs of the Länder and Gemeinden including public corporations shall further be permissible if the data are an essential prerequisite to enable the recipient to fulfil the tasks entrusted to him by law.

(3) Data may be transmitted to other recipients than mentioned in p. 2 only, if it is necessary for the safeguarding of justified interests of a third party, which prevail the interest of the data subject that his personal data are kept secret. In case of doubt priority shall be given to the confidentiality of the personal data.

(4) Transmissions which are not registered have to be recorded in such a way, that the data subject can be given information according to sec. 11. Transmissions as defined in sec. 8 p. 3 do not need to be recorded.

Notification of data processing and transmission

Sec. 8. (1) Every data controller shall at the beginning of data processing submit a notification to the Data Processing Register (sec. 47).

(2) This notification shall contain the name, the address and the registration number of the data controller - if it has already been attributed - , the purpose of the notified processing, its legal basis, the groups of data subjects affected by the processing as well as the classes of their data. Transmissions of data shall be notified according to sec. 23 p. 2, numbers 2 and 5.

(3) Types of data processing and transmissions, which are performed by a great number of data controllers and the contents of which are defined by law or by a contract with the data subject, may be exempted from mandatory notification by an order of the Federal Chancellor, which may be passed according to the detailed provisions of sec. 23 p. 4 after consultation of the Data Protection Council. If such data processing is made, only the name, the address and the registration number of data controller - if it has already been attributed - as well as the denomination of the standard type of data processing shall be notified to the Data Processing Register.

(4) P. 1 to 3 shall apply mutatis mutandis to changes of notified facts.

(5) The data controller shall use the registration number, which is attributed to him in case of registration whenever he transmits data and gives information to the data subject.

Registration

Sec. 8a. (1) If a notification is incomplete in the sense of p. 2, the Data Processing Register may within two months instruct the data controller to complete it within an adequate prescribed period of time.

(2) A notification is incomplete, if elements are missing, incorrect, inconsistent or so insufficient that people looking into the register will - when exercising their rights on the basis of this law - not obtain sufficient information, whether or not the data processing infringes their privacy interests. Inconsistency is given, if the contents of notified processing are not covered by its notified legal basis.

(3) If the Data Processing Register in examining the notification finds that - due to the lack of a legal basis for the data processing - privacy interests of data subjects, that need protection, are endangered, the Data Protection Commission shall be informed. If the Data Protection Commission shares the concerns of the Data Processing Register, it shall communicate them to the highest competent administrative body.

(4) If the Data Processing Register's instruction to complete a notification is not complied with in due time, the Register shall submit the notification to the Data Protection Commission. The defects shall be substantiated. If the Commission finds that the

notification is incomplete, registration shall be refused. Otherwise the Data Processing Register shall be instructed to register.

(5) Further provisions for the registration are to be found in sec. 23b.

Data Protection Order

Sec. 9. (1) The supreme organs of the Federation and the Länder shall, without prejudice to the provisions of p. 2, issue after consultation of the Data Protection Commission a Data Protection Order for each data controller under their supervision, in which - depending on the kind of data - the principles for their collection, processing, use and the conditions for the greatest possible protection of personal data shall be stated.

(2) Autonomous or semi-autonomous bodies shall, to the extent they process, transmit and commit data issue a Data Protection Order in accordance with p. 1. That order shall be subject to approval by the supervisory authorities. The supervisory authorities shall consult the Data Protection Commission. Approval shall be given if the order complies with the statutory provisions.

Data security measures

Sec. 10. (1) For all organisational parts of a data controller or a data processor, who are using data, measures for data protection have to be taken. According to the quality of the data used, to the extent and purpose of the application and under consideration of technical possibilities and of economic reasonability those measures have to ensure that data are used lawfully and protected from unauthorised access.

(2) Insofar as it is necessary for the fulfilment of the second sentence of p. 1,

1. the competences for the application of data shall be explicitly distributed among subdivisions and employees,
2. the application of data must be subject to orders of the competent subdivisions or employees,
3. each employee has to be informed about his duties according to this law and in particular to the regulations on data security,
4. access to the rooms of the data controller and the data processor shall be regulated,
5. authorisation for the access to data and programs and the protection of storage media from unauthorised access or use shall be regulated,
6. the authorisation to the use of computers shall be defined and each computer has to be protected from unauthorised use by the hardware and software used,
7. the necessary data security measures shall be checked; for this purpose protocols must be kept, which enable authentication of the steps of processing.

(3) Prescriptions for data security shall be passed and made available in such a way, that all employees at any time can inform themselves about the actual prescriptions.

Right of access

Sec. 11. (1) A data subject shall on proof of his identity and on written request to the data controller be informed in writing within four weeks and in a generally understandable form about his data, their origin and the legal basis for their collection, processing, use and transmission, unless such data - due to law or administrative order and in the case of

prevailing public interest - must not be disclosed even to the data subject. If data are or have been transmitted, the data subject shall may also require information on the recipient.

(2) The data subject shall cooperate in this process. He has to specify the EDP which may concern him or give due reason for his belief that the files of the data controller contain his data because of error or abuse.

(3) If a request under p. 1 is rejected as a whole or partly, the data subject must be informed in writing and with reasons for this rejection.

(4) The information under p. 1 must be given free of charge if it concerns current files and if the data subject in the context of this purpose has not yet exercised his right of access in the current year. In all other cases the Data Protection Order may - after consultation of the Data Protection Council - prescribe a lump sum for cost compensation. The amount of the compensation must be fixed so as to cover the costs actually arising from the request for information. The request may be refused, if the data subject does not cooperate according to p. 2 or does not pay the prescribed cost compensation. Paid compensations must be refunded without prejudice to further claims for damages, if data have been used illegally or if the access has led to rectification of the data.

Obligation to rectify or delete data

Sec. 12. (1) Any data controller shall without delay, but not later than two weeks after establishing the factual basis for the processing of data, rectify (delete) or have rectified (deleted) data which are incorrect or have been collected or processed in violation of sec. 6. If due to economic reasons physical deletion or rectification of exclusively machine-readable data are only appropriate at fixed times, such data must in the meantime be deleted or rectified logically.

(2) Rectification or deletion according to p. 1 shall be carried out or initiated,

1. ex officio, or
2. upon reasoned request from the data subject, or
3. in pursuance of a decision of the authority competent for the establishment of the data, or
4. in pursuance of a decision of the Data Protection Commission, or
5. in pursuance of a decision of the Administrative Court.

(3) If the facts underlying the processing of data have not been established within twelve weeks after the request, the applicant shall be informed of this immediately in writing.

(4) If the request from a data subject is rejected, he shall be informed of this in writing within four weeks.

(5) The burden of proof for the correctness of the data shall lie with the data controller unless the data were collected on the basis of information exclusively supplied by the data subject.

(6) If the rectification or deletion of the data has been carried out upon request from the data subject or in pursuance of a decision of the Data Protection Commission, the data subject and in the latter case, the Commission also shall be informed by the data controller.

(7) If data rectified or deleted according to p. 1 have been transmitted prior to rectification or deletion, the data controller has to inform the recipient of such data if the data subject so demands, if he can prove credibly a justified interest and if the recipient can still be ascertained.

(8) Rectification and deletion shall be excluded if the data were correct and complete at the time of collection and if the purpose for which they were collected or processed excludes modification of the data according to changes in the facts underlying them.

(9) If rectification or deletion is made on the basis of a decision of the authority competent for the establishment of the data, the data controller shall be bound by that decision.

(10) In case of transmission and use of data, which are disputed by the data subject as far as their correctness is concerned, the data subject may require that the dispute be noted, if neither the correctness nor the incorrectness can be established. The data controller may apply to the Data Protection Commission to decide whether such a note is to be maintained.

Service in data traffic

Sec. 13. (1) Data controllers entitled to collect or process data according to sec. 6 may consult service processors for their EDP, if this is necessary for practical or economic reasons and provided that the interests of the data subject warranting protection or public interests are not opposed to this.

(2) In the absence of special legal provisions for the duties of service processors, sec. 19 applies to processors within the private sector and mutatis mutandis to processors within the public sector.

(3) The Data Protection Commission must be informed of an intended consultation of a service processor except in cases where such consultation is explicitly provided for by law, or where the service processor is an organisation which is superior or subordinated to the data controller himself or to an institution superior or subordinated the data controller. If the Data Protection Commission decides that interests of the data subject warranting protection or public interests are opposed to consultation of a service processor, it has to inform the data controller without delay.

Remedies for the data subject

Sec. 14. (1) The Data Protection Commission shall decide on violations of the provisions of this law and of the implementation provisions based thereon, insofar as the complainant claims that his rights have been violated, as well as on applications under p. 3.

(2) In case of imminent danger to the rights of the complainant, the Data Protection Commission may prohibit the use or transfer of data or specific data processing operations.

(3) If in administrative proceedings using processed data the violation of provisions of this law or of implementation provisions based thereon is claimed, administrative proceedings shall be suspended - unless delay might cause damage - until the Data Protection Commission has decided. Such a decision shall be applied for immediately.

Ex officio proceedings

Sec. 15. (1) Where proceedings under sec. 14 prove that the rights of other persons granted in this law or in the implementing provisions based on it were violated, such violation shall be officially stated by the Data Protection Commission, which decision shall be communicated to the data controller and service processor. The decision shall be published by the Data Protection Commission in the Amtsblatt (Official Gazette) of the Wiener Zeitung.

(2) The data controller or service processor shall comply with the decision of the Data Protection Commission within an appropriate period fixed by the Commission.

Combination of proceedings

Sec. 16. If efficiency, speed, simplicity and cost-effectiveness so require, the Data Protection Commission shall combine proceedings concerning the same data controller or service processor.

PART 3
Private Sector
Permissibility of collection and processing

Sec. 17. (1) Data may be collected and processed by a person not mentioned in secs. 4 or 5 only if the contents and the purpose of this data processing are covered by legitimate tasks and if the interests of the data subject that need protection, in particular as regards the respect of his privacy and family life, are not infringed.

(2) Data may be processed for exclusively private purposes, if the data subject has given them to the data controller or if the data controller in his private sphere has received them in some other legal way, in particular in accordance with secs. 7 or 18.

Permissibility of transmission

Sec. 18. (1) The transmission of data which have been collected and processed according to sec. 17 p. 1 shall be permissible only if

1. the data subject has expressly and in writing agreed to the transmission, which consent may be revoked in writing, or
2. the transmission is part of the legitimate tasks of the person, or
3. the transmission is necessary for the safeguarding of prevailing justified interests of third persons.

(2) The transmission of data which have been processed according to sec. 17 p. 2 shall only be permissible with the consent of the data subject.

(3) P. 1 and 2 shall not apply in cases of a legal obligation for transmission.

(4) Existing obligations for confidentiality shall not be affected by the permissibility of transmission according to p. 1 or 2.

(5) Transmissions which are not registered shall be recorded in such a way that a data subject can gain access as granted in sec. 25. Transmissions according to sec. 23 p. 4 do not require recording.

Service in data traffic

Sec. 19. Service processors may only use data for the data controller according to the following obligations:

1. data may only be used within the mandate of the data controller; in particular the unauthorised transmission of data is forbidden;

2. all security measures defined in sec. 21 shall be taken; in particular the data processing must be performed only by employees, who - according to sec. 20 - have committed themselves data confidentiality;

3. in case of an intended consultation of a further service processor the data controller must be informed in such time that he can prohibit such consultation;

4. in cases where it might - due to the character of the service - be appropriate, all necessary technical and organisational measures for the performance of the controller's duties to grant access, to rectify and to delete must be taken in consultation with the data controller;

5. after the end of the service all results of service processing and all documents containing data must be transmitted to the data controller or according to his mandate be destroyed or kept for him;

6. the data controller shall be given all information necessary to control the compliance with the obligations mentioned in p. 1 to 5 above.

Confidentiality of data

Sec. 20. (1) Automatically processed data which have been entrusted or made accessible within employment relations may, without prejudice to other obligations to confidentiality, only be transmitted on the basis of the express instruction of the data controller, the employer or their representatives (confidentiality of data).

(2) Data controllers and service processors shall conclude contracts with their employees, where those explicitly stipulate the transmission of automatically processed data only on the basis of instructions according to p. 1 and keep the data confidential even after the end of the contractual relationship to the data controller or service processor.

(3) The employer shall be responsible for the completeness and the lawfulness of instructions concerning transmission of data and for providing sufficient information to the employees about these instructions.

(4) The refusal of an employee to carry out an instruction infringing sec. 18. may not lead to any detriment of the employee.

(5) Nobody is entitled to invoke the confidentiality of data as a reason for withholding testimony in official proceedings.

Measures of data security

Sec. 21. Data controllers and service processors within the private sector shall undertake all necessary measures of data security as prescribed by sec. 10.

Notification of data controllers

Sec. 22. (1) Every data controller processing data according to sec. 17 p. 1 shall, when beginning with data processing, notify his name (other designation), his address and his legitimate task for registration and to submit such documents which are necessary to substantiate this. Modifications of these data shall be notified without any delay.

(2) If the data controller performs standardised processing (sec. 23 p. 4) he shall in addition notify which cases of standardised processing he performs.

(3) The data controller shall use the registration number (sec. 23b p. 2), which is attributed to him in the case of registration, whenever he transmits data or gives information to the data subject.

Notification of data processing and transmission

Sec. 23. (1) Data controllers shall, except in the cases mentioned in p. 4, at the beginning of a specific data processing notify it to the Data Processing Register for registration.

(2) This notification shall contain:

1. the name (other designation) and the address of the data controller;
2. the registration number of the data controller, if it has already been attributed to him;
3. the purpose of the notified processing;
4. the groups of data subjects affected by the processing as well as the classes of their data;
5. - if data transmissions are envisaged - the groups of data subjects affected by the transmission as well as the classes of their data which shall be transmitted and - if transborder transmission is envisaged - the recipient country;
6. if a licence for transborder data flow according to secs. 32 to 34 had to be applied for - the file number of the Data Protection Commission's licence.

(3) P. 1 and 2 shall apply mutatis mutandis to changes in notified data processing.

(4) Types of data processing and transmissions, which are performed by a great number of data controllers and the contents of which are defined by law or by a contract with the data subject, may be declared as standard types of processing by an order of the Federal Chancellor. These standard types of processing are exempted from mandatory notification. The order may in exceptional cases retain mandatory notification if this is necessary for the protection of the privacy interests of data subjects.

Proceedings for notification of defects

Sec. 23a. (1) If a notification is incomplete in the sense of p. 2, the Data Processing Register may within two months instruct the data controller to complete it within an adequate prescribed period of time.

(2) If on examining the notification the Data Processing Register finds that - due to the lack of a legal basis for the data processing - the privacy interests of data subjects, that need protection, are endangered, the Data Protection Commission shall be informed. If the Data Protection Commission shares the concerns of the Data Processing Register, it shall order by decree the provisional suspension of the data processing or of parts of it.

(3) Decrees according to p. 2 expire with the end of the procedure mentioned in p. 4, but in any case after 6 months at the latest.

(4) If the Register's instruction to complete a notification is not complied within due time, the Register shall submit the notification to the Data Protection Commission. The defects shall be substantiated. If the Commission finds that the notification is incomplete, registration shall be refused and further data processing shall be forbidden. Otherwise the Data Processing Register shall be instructed to register.

Registration

Sec. 23b. (1) Notifications according to secs. 8, 22 and 23 shall be registered in the Data Processing Register, if

1. within two months after notification no instruction to complete the notification is given,

2. the data controller completes the notification according to the instructions in due time, or

3. the Register has been instructed by the Data Protection Commission to do so.

(2) The data controller shall be informed about the registration in writing; his extract from the Register shall be attached. The information shall contain the registration number that has been attributed to him.

(3) The registration in no ways can prejudge a decision of the competent authority on the lawfulness of a specific data processing.

(4) Erasures and alterations in the Data Processing Register may take place on request of a registered person or in pursuit of a decree of the Data Protection Commission according to p. 5.

(5) If the Data Processing Register obtains subsequent information about facts, which cause the incompleteness of registrations, it has to start proceedings for notification of defects ex officio. Sec. 23a is applicable, but the Data Protection Commission may order by decree a rectification if names or addresses have been changed. The proceedings for notifications of defects shall be noted in the Register until they are finished.

(6) The Federal Chancellor shall - after consultations of the Data Protection Council - pass an order with detailed regulations for the registration. Transparency of registrations and simplicity of access to the Register shall be considered in this context.

Registration fee

Sec. 24. (1) For the use of the Data Processing Register according to secs. 22 and 23a a fee shall be payable; the payment shall be established together with the notification. The Federal Chancellor shall - after consultation of the Data Processing Council - regulate the modalities of payment by order. The amount of the fee is AUS 700,-- for a first notification which does not contain exclusively standard types of data processing, and AUS 150,-- for a notification of changes and for a notification, which exclusively contains standard types of data processing.

(2) The registration fee may be prescribed by decree of the Data Protection Commission, if the payment is not established together with the notification.

(3) Notifications which aim at the complete erasure of a data subject from the register or which only contain changes of name and address of the data subject are free from charge.

Right of access

Sec. 25. (1) A data subject shall on proof of his identity be informed by the data controller about his data and their origin. If these data have been transmitted, the data subject shall in addition be informed about the recipient. The information shall be given within four weeks in writing and in a generally understandable form, if the data subject is not satisfied with oral information. If the data subject agrees, instead of written information direct access with the possibility of making printouts or copies may be given.

(2) If data are processed according to sec. 19, information about the name and address of the service processor shall be given.

(3) The data subject shall cooperate in this process. He has to specify the EDP which may concern him or render credible that the files of the data controller contain his data because of error or abuse.

(4) The information under p. 1 must be given free of charge if it concerns current files and if the data subject in the context of this purpose has not yet exercised his right of access in the current year. In all other cases the Data Protection Order may - after consultation of the Data Protection Council - prescribe a lump sum for cost compensation. The amount of the compensation must be fixed so as to cover the necessary costs actually caused by the request for information. The request may be refused, if the data subject does not cooperate according to p. 3 or does not pay the prescribed cost compensation. Paid compensations must be refunded without prejudice to further claims for damages, if data have been used illegally or if the access has led to rectification of the data.

(5) Legal obligations for secrecy shall remain undisturbed.

(6) Information may not be given if it endangers prevailing justified interests of the data controller or of third parties and if the reasons are communicated to the data subject.

(7) If a request under p. 1 is rejected as a whole or partly, the data subject must receive written and reasoned information on this rejection within four weeks.

(8) From the moment when a data controller receives a request for access he may not delete those data within a time-frame of four months or before the final judicial decisions, except in cases, where deletion is performed regularly and has been initiated in advance.

Obligation to rectify data

Sec. 26. (1) If for reasons of efficiency data stored on an exclusively automatically readable data medium can be rectified physically only at specific times, such data shall first be rectified logically and then physically at such times.

(2) In the case of transmission and use of data, which are disputed by the data subject as far as their correctness is concerned, the data subject may require a note concerning the dispute to be added to the data, if no agreement as to the correctness of data can be achieved. Such a note may only be deleted with the consent of the data subject or on the basis of a final judicial decision. If the request for rectification (p. 1) is brought before a court and rejected, the judgement shall on request of the data controller declare that the note be deleted. The data controller may appeal to court for the deletion of the note concerning the dispute, if he can prove the correctness of the data (Sec. 12 p. 5).

Obligation to delete data

Sec. 27. (1) Data shall be deleted,

1. if their collection or storage is illegal; or

2. on request from the data subject, if their collection or storage is no longer necessary for the purposes of EDP and unless the deletion is contrary to prevailing and justified interests of the data controller or a third party or to a statutory obligation to keep the data.

(2) If for reasons of efficiency data stored on an exclusively automatically readable data medium can be rectified only at specific times, such data shall first be rectified logically and then physically at such times.

Liability

Sec. 28. (1) Rights arising from Part 3 of this law may be enforced against persons who are not mentioned in secs. 4 and 5 before the ordinary courts.

(2) If data are processed, used or transmitted in violation of this law or of implementing provisions based on it, the data subject may, without prejudice to other claims for damages, demand abolition of and abstention from such a violation.

Civil proceedings

Sec. 29. (1) Original jurisdiction in respect of actions filed in accordance with this Federal Act shall lie with the Regional Court competent for civil matters of the Land where the data subject has his ordinary residence or headquarters. The data subject may bring an action also before the Regional Court of the Land where the data controller or the service processor has his ordinary residence or headquarters.

(2) Actions filed in accordance with this Federal Act in respect of labour issues within the meaning of sec. 50 of the Federal Law on the Jurisdiction of Labour and Social Courts, Federal Law Gazette No. 104/1985, shall be subject to the said law; as far as jurisdiction is concerned, however, p. 1 shall be applied muis hd muindits.

PART 4
Transborder Data Flow

Transborder transmission and committing of data

Sec. 32. (1) Transmission and committing of data into countries with data protection regulations equivalent to Austrian law does not require a licence from the Data Protection Commission. An Order issued by the Federal Chancellor after consultation of the Data Protection Council shall state to which extent such equivalence exists.

(2) Transborder transmissions and committings do not require a licence, if

1. they take place according to national or international legal provisions which explicitly mention the classes of transmitted or committed data and the recipients, or

2. if the data subject asked for the transmission in writing, which request may be revoked in writing, or

3. if the data have been published legally in Austria, or

4. if the transmissions or committings are such as exempted from licensing by an order of the Federal Chancellor after consultation of the Data Protection Council, because they are performed by a great number of data controllers and the contents of which are defined by law or by a contract with the data subject and if no privacy interest of data subjects, that need protection, require examination by the Data Protection Commission (standard transmissions and standard committings).

(3) Transborder transmission or committing may be exempt from licensing only if secs. 6, 7, 17 and 18 have been complied with and if - in case of transborder committing - written stipulation of the service processor exists that he will comply with the duties enumerated in sec. 19.

Licence for transborder transmissions

Sec. 33. (1) In all cases not mentioned in sec. 32 transborder transmissions of data require a preceding licence of the Data Protection Commission.

(2) The licence shall be refused, if

1. the processing, from which the transborder transmission should take place, is illegal, or

2. if the prerequisites of secs. 7 or 18 are not fulfilled, or

3. if privacy interests of data subjects which need protection might be endangered by the transborder data flow, or

4. if public interests or obligations of international law are opposed to it.

(3) The Data Protection Commission shall transmit a copy of each decree, by which a transborder transmission is licensed, to the Data Processing Register; this copy shall be attached to the registration file.

Licence for service processing outside the country

Sec. 34. (1) In all cases not mentioned in sec. 32 transborder committing of data for the purpose of service processing requires a preceding licence of the Data Protection Commission.

(2) The licence shall be refused, if

1. the processing, from which the transborder transmission should take place, is illegal, or

2. if the foreign service processor did not stipulate to the applicant that he will comply with the duties enumerated in sec. 19, or

3. if privacy interests of the data subjects which need protection might be endangered by the transborder data flow, or

4. if public interests or obligations of international law are opposed to it.

(3) The Data Protection Commission shall transmit a copy of each decree, by which a transborder committing is licensed, to the Data Processing Register; this copy shall be attached to the registration file.

PART 5
Data Protection Commission, Data Protection Council and Data Processing Register

Supervisory bodies

Sec. 35. (1) Without prejudice to the jurisdiction of Ordinary Courts a Data Protection Commission as well as a Data Protection Council shall be established to safeguard data protection according to this law.

(2) The management of the bodies mentioned in p. 1 shall be the responsibility of the Federal Chancellor's Office. The Federal Chancellor shall on the proposal of the Data Protection Council provide the staff required for these bodies. In the execution of their duties, the members of the staff shall receive their instructions from the chairman or such members of the bodies as specified in their rules of procedure.

Competence of the Data Protection Commission

Sec. 36. (1) (Constitutional provision) The Data Protection Commission shall decide:

1. on complaints of persons who claim a violation of their rights according to this law and of implementation provisions based thereon through the acts of an organ that would fall under Part 2 of the data protection act, if automated data processing had been employed, inasfar as these acts are not the acts of a court;

2. ex officio, if during proceedings according to No. 1 the rights of other persons are found to have been violated in a like manner;

3. on the duty of a data controller falling under Part 2 to maintain a note of dispute;

4. on cases relating to entries into the Data Processing Register;

5. on licenses necessary for transborder data flow;

6. on appeals against decisions under sec. 50.

(2) In addition, the Data Protection Commission shall be competent in all other matters delegated to it by law, in particular its rights according to secs. 9, 13, 29, 44 and 52, decisions according to sec. 29 p. 3 and sec. 38 p. 6 and resolutions according to secs. 39 p. 2 and secs. 45, as well as recommendations according to sec. 41 and the activities report according to sec. 46.

Effect of decisions

Sec. 37. (1) If the Data Protection Commission states a violation of this law or of implementing provisions based on it, administrative authorities shall be obliged to create without delay and with all legal means available a situation corresponding to the legal opinion of the Data Protection Commission. The decision of the Data Protection Commission shall specify the authority responsible for its execution. The execution procedure shall be governed by the provisions normally applicable to this authority.

(2) There shall be no appeal against decisions of the Data Protection Commission. They may not be set aside or modified in an administrative procedure.

(3) Complaints may be brought before the Administrative Court (Verwaltungsgerichtshof).

Composition of the Data Protection Commission

Sec. 38. (1) The Data Protection Commission shall consist of four members appointed by the Federal President on the proposal of the Federal Government for a period of five years. Members may be reappointed. One member shall be a judge. Members shall have experience in the field of data protection.

(2) The proposal of the Federal Government for the appointment of the members of the Data Protection Commission shall be prepared by the Federal Chancellor. He shall have regard to the following proposals:

1. three names proposed by the President of the Supreme Court of Justice for the judicial member;

2. two members proposed by the Länder.

(3) One proposed member shall be a lawyer from the Federation's civil service.

(4) For every member a substitute member shall be appointed. The substitute member shall take the place of the member if the latter is unable to fulfil his duties.

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

1. members of the Federal Government or of a Land Government or Secretaries of State;

2. persons directly concerned with the processing of data covered by the provisions of this law;

3. persons not eligible for the National Assembly.

(6) Where a member of the Data Protection Commission fails, without adequate excuse, to respond to notifications of three consecutive meetings or if one of the grounds for exclusion specified in p. 5 subsequently covers him, the Data Protection Commission shall, after hearing the member concerned, decide on this accordingly. Such a decision shall entail 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 two members.

(7) P. 2, 3, 5 and 6 shall apply to substitute members mutatis mutandis.

(8) Where membership ceases before the expiration of a member's term of office by reason of death, voluntary resignation or in accordance with p. 6, the respective substitute member shall become a member of the Data Protection Commission and a new substitute member shall be appointed in accordance with p. 2 and 3 for the remainder of the term of office.

(9) The members of the Data Protection Commission shall be entitled to claim their travel expenses (cost scale 5) in accordance with the rules applicable to federal civil servants in the general administration. They shall also be entitled to remuneration for the time and effort they devote to their duties, to be determined by the Federal Government by Order on the proposal of the Federal Chancellor.

Chairmanship and Secretariat of the Data Protection Commission

Sec. 39. (1) The judge shall take the chair of the Data Protection Commission.

(2) (Constitutional Provision) The Data Protection Commission shall issue its own rules of procedure in which one of its members shall be entrusted with conduct of current business which may also include procedural decisions.

(3) A decision of the Data Protection Commission shall require a majority of votes. In the case of a split vote the Chairman shall have the final decision. Members shall not be entitled to abstain from voting.

(4) Decisions of the Data Protection Commission that are of general interest to the public shall be made public in an appropriate way. The Data Protection Commission shall decide on all further modalities regarding the publication of decisions.

Independence of members of the Data Protection Commission

Sec. 40. (Constitutional Provision) The members of the Data Protection Commission shall in the exercise of their duties be independent and not bound by any instructions.

Recommendations of the Data Protection Commission

Sec. 41. If the Data Protection Commission doubts the legality of collection, processing, use or transmission of data for or on behalf of persons or entities under secs. 4 or 5, it shall inform the highest administrative body responsible for the processing in question of such doubts together with its reasons and recommendations how to establish a lawful situation. The body concerned shall within a reasonable time, which shall in no case exceed 12 weeks, either comply with the recommendations and inform the Data Protection Commission, or provide a written explanation of the reasons why the recommendations have not been complied with.

Competence of the Data Protection Council

Sec. 42. (1) The Data Protection Council shall - in addition to the competences mentioned in secs. 4, 5, 8, 11, 22, 23, 23b, 24, 32, 35, 44, 45, 46, 47 and 52 - be competent for the following matters:

1. requiring information and reports from the competent bodies about issues of data protection within the public sector;

2. observing the effects of automated data traffic on the protection of interests that need protection, in particular as privacy and family life under sec. 1 of this law is concerned, and attaching the results of such observations to the report of the Data Protection Commission under sec. 46 p. 1 as well as any EDP-reports and plans of the Federal Government;

3. making proposals to the Federal Government, the Land Government and through them to the legislative bodies, concerning possible improvements for data

protection, which are necessary for the protection of constitutional rights because of the development of data traffic;

4. considering upon request of a representative of a political party who is a member of the Data Protection Council questions of fundamental importance to data protection;

5. establishing its own rules of procedure.

(2) The competent Federal Ministers and Land Governments shall upon request of the Data Protection Council provide it with information about their experience in the field of data protection in their particular spheres.

(3) Court decisions and settlements in proceedings under this law shall be communicated to the Data Protection Council.

Composition of the Data Protection Council

Sec. 43. (1) The Data Protection Council shall consist of:

1. representatives of the political parties: the greatest party in the Main Committee of the National Assembly shall send four representatives, the second party three representatives and every other party represented in the Main Committee of the National Assembly shall send one representative to the Data Protection Council. Where there is equality of seats between the major parties in the National Assembly each of these parties shall send three representatives;

2. one representative each from the Austrian Chamber of Labour and the Federal Chamber of Commerce;

3. two representatives of the Länder;

4. one representative each from the Gemeindebund (local authorities of federation) and the Städtebund (federation of towns);

5. a representative of the Federation to be appointed by the Federal Chancellor.

(2) The representatives referred to in p. 1 No. 3, 4 and 5 shall have experience in data processing within public administration.

(3) For every member a substitute member shall be designated.

(4) Sec. 38 p. 5 shall apply mutatis mutandis.

(5) Membership of the Data Protection Council shall continue until the time when other representatives are nominated by the bodies with nominating power (p. 1).

(6) Membership of the Data Protection Council is honorary. Members of the Data Protection Council who live outside Vienna shall, where they participate at meetings of the Council, be entitled to reimbursement of travel expenses (cost scale 5) in accordance with the rules applicable to federal civil servants in the general administration.

Chairmanship and Secretariat of the
Data Protection Council

Sec. 44. (1) The Data Protection Council shall choose from amongst its members a chairman and two vice-chairmen. The term of office of the chairman (chairmen) shall be five years, irrespective of changes in the membership under sec. 43 p. 5. Such persons may be reappointed for further terms of office.

(2) Meetings of the Data Protection Council shall be convened when necessary. Where a member or the Data Protection Commission so requires, the Chairman shall convene a meeting which shall take place within four weeks.

(3) Deliberations and decisions of the Data Protection Council shall require a quorum of more than half of the members. Decisions shall be made by a simple majority of votes. In the case of a split vote the Chairman shall have the final decision. Members may not abstain from voting.

(4) The adjunction of dissenting opinions is possible.

(5) The Data Protection Council may form among its members standing or ad hoc working parties which may be entrusted with the preparation of expert appraisement and conduct of individual cases. It may also entrust the management, preliminary expert appraisement and conduct of individual cases to an individual member (the rapporteur).

(6) Every member of the Data Protection Council shall - expect where he has a justifiable excuse - attend the meetings of the Council. Members shall give due notice of their inability to attend, whereupon the substitute member shall be invited.

(7) Members of the Data Protection Commission who are not members of the Data Protection Council shall be entitled to attend meetings of the Council or its working parties. They shall have no right to vote at such meetings.

Provisions Common to the Data Protection Commission and the Data Protection Council

Sec. 45. (1) (Constitutional Provision) All administrative bodies or entities covered by sec. 4 and 5 shall give the Data Protection Commission and the Data Protection Council all necessary assistance in the performance of their duties, shall enable them to inspect documents, data media and other facilities concerned with the collection, processing and transmission of data and shall on request provide the appropriate information.

(2) (Constitutional Provision) The deliberations of the Data Protection Commission and the Data Protection Council shall be confidential. The two bodies may waive the confidentiality where this is deemed necessary having regard to the subject matter and aims of the deliberations and where confidentiality is not required in the public interest or in the interest of a party.

(3) The Data Protection Commission and the Data Protection Council may - where appropriate - invite experts to take part in their deliberations on specific issues.

(4) The Federal Chancellor shall convene the first meetings of the Data Protection Commission and the Data Protection Council. In the Data Protection Council the chair shall be taken by the oldest member until the election of a chairman.

Data Protection Reports

Sec. 46. (1) Every two years the Data Protection Commission shall draw up a report on its activities as well as the experiences gained with them and transmit this report to the Data Protection Council.

(2) The Data Protection Council shall upon receiving the report of the Data Protection Commission draw up a report on the development of data protection in Austria (Data Protection Report) and transmit it together with the report of the Data Protection Commission and a report on the activities of the Data Processing Register to the Federal Chancellor.

(3) The Federal Chancellor shall submit the Data Protection Report to the National Assembly together with the attached documents, with comments from the Federal

Government, with a report on the international development of processing and protection of data, and with possible recommendations. As far as the report deals with data processing of the Länder (sec. 5) the Federal Chancellor shall transmit the Data Protection Report to the Länder.

Data Processing Register

Sec. 47. (1) A Data Processing Register shall be established at the Austrian Central Office of Statistics and shall be managed according to the instructions of the Federal Chancellor.

(2) The Register is open to the public. Access to the Data Protection Commission's licences for transborder data flow, which are deposed together with the registrations, shall only be given, if the applicant for the access substantiates that he is subject of the licensed transmission or committing, and only if no prevailing interests of the data controller or third parties in keeping those information secret are opposed to this.

(3) Copies from the register, which serve a data subject in the pursuit of his rights, shall be given free of charge.

(4) The Federal Chancellor shall - after consultation of the Data Protection Council - pass an Order with detailed regulations for the management of the Register.

PART 6
Penal Provisions
Breach of secrecy

Sec. 48. (1) Any person illegally disclosing or utilising data, which have been entrusted or made accessible to him exclusively because of his professional occupation with data processing, and the disclosure or utilisation of which may violate justified interests of the data subject shall be punished by court with imprisonment for up to one year unless a more severe penalty is envisaged by another legal provision.

(2) Prosecution shall require an application of a person whose interest in privacy has been violated, or an application of the Data Protection Commission.

(3) The general public shall be excluded from the oral hearing, if

1. the public prosecutor, the defendant or any private party so require, or if

2. the court considers it necessary to safeguard the interests of third persons.

Unauthorised intervention with data traffic

Sec. 49. Any person illegally causing damage to the rights of others by acquiring automatically processed data shall be liable to punishment by a court of up to one year of imprisonment, unless the offence carries a higher penalty under another legal provision.

Administrative penal provision

Sec. 50. (1) Any person who processes data without having complied with his duties for notification or licensing, or continues data processing though it has been prohibited by the Data Protection Commission according to sec. 23a p. 2, or transfers data in contravention of sec. 8 p. 5 or sec. 22 p. 3, shall be guilty of an administrative offence punishable by a fine of up to AUS 150,000,--.

(2) The attempt shall be punished.

(3) The forfeit of data carriers and program may be imposed (secs. 10, 17 and 18 VStG - Administrative Penal Code of 1950) if such objects form part of an administrative offence under p. 1.

(4) The competence for decisions under p. 1 to p. 3 shall lie with the Landeshauptmann.

(5) The Administrative Penal Code of 1991 (Verwaltungsstrafgesetz 1991) shall be applied to the proceedings of the Data Protection Commission as appeal instance (sec. 36 p. 1 No. 6) against decisions according to p. 4 with the exception that in Part 5 the Data Protection Commission shall be competent according to sec. 39 instead of the Independent Administrative Tribunal (Unabhängiger Verwaltungssenat) or one of its Divisions or its competent member.

(6) Final decisions under p. 4 shall be communicated to the Data Protection Commission.

Sec. 51. Abrogated pursuant to Art I p. 34 of the 1986 amendment of the Data Protection Act.

Testing of new working methods and techniques of the public administration

Sec. 52. (1) The provisions of secs. 8 and 9 shall not apply to applications as far as they are used by the legal entities referred to in secs. 4 and 5 for testing new working methods and techniques of the public administration before they are generally introduced.

(2) Ordinances shall be issued for measures within the meaning of p. 1 after consultation of the Data Protection Commission and the Data Protection Council. Such ordinances shall take due account of the principles of the expediency and efficiency of the public administration and shall specify the subject matter and the area of application of pilot schemes pursuant to p. 1 as well as the type and use of the data. Ordinances shall be restricted to a specified period which is to be fixed in accordance with the time required for the assessment of the pilot scheme.

(3) Ordinances within the meaning of p. 2 shall be issued:

1. for applications within the sphere of the Bund (sec. 4) by the competent Federal Minister or the Federal Government;

2. for applications within the sphere of the Länder (sec. 5) by the Land Governments.

Applicability of Sec. 7 in respect of administrative matters as provided by Art. 30 of the Federal Constitution

Sec. 53. Sec. 7 shall apply to data pertaining to administrative matters assigned to the President of the National Assembly under Art. 30 of the Federal Constitution, subject to the proviso that unless the data subject has given his consent explicitly in writing, such data may be transmitted only with the approval of the President of the National Assembly.

Transitional provisions and final clauses Exception for mass media

Sec. 54. From all non-constitutional provisions of this law only secs. 19 to 21 shall apply to the collection, processing, use, transmission or committing of data for automated processing, if this is done by mass media enterprises or mass media services for their journalistic activities.

Exemption from fees and duties

Sec. 56. All applications of data subjects for the safeguarding of their rights which are based on this law and all applications in the registration procedure as well as the experts from the register according to sec. 23b p. 2 are exempted from all stamp duties and fees imposed by the Federation.

(Translator's Note: **Sec. 57 and 58** contain only legal technicalities about the Data Protection Act's entry into force which are meaningless to anyone not involved with the direct application of the law.)

Execution

Sec. 59. The execution of this Federal Act is entrusted to the Federal Chancellor and the other Federal Ministers within their spheres of competence, unless such execution rests with the Federal Government or the Land Government.