Austria

Dr Ferdinand Graf, Graf & Pitkowitz Rechtsanwälte GmbH

www.practicallaw.com/3-385-8573

REGULATION

1. What national law(s) apply to the collection and use of personal data? If applicable, has Directive 95/46/EC on data protection (Data Protection Directive) been implemented?

The applicable Act in relation to collecting and using personal data in Austria is the Data Protection Act 2000 (*Datenschutzgesetz 2000*) (DSG). It is based on the Data Protection Directive.

2. To whom do the rules apply (EU: data controller)?

The right to data protection is a constitutional civil right which applies to everyone including natural persons, (public or private) legal entities and associations (referred to as data subjects).

3. What data is regulated (EU: personal data)?

The DSG regulates personal data, that is, information about an identified or an identifiable person.

"Sensitive data" is subject to stricter rules. Sensitive data is considered to be information about a person relating to:

- Racial or ethnic origin.
- Political opinions.
- Trade-union membership.
- Religious or philosophical beliefs.
- Health.
- Sex life.

If not otherwise stated, the following explanations refer to regular personal data. The special provisions for sensitive data are mentioned separately (*see Question 11*).

The DSG also contains special provisions about "indirect data". This refers to personal data if the identity of the data subject can be retraced, but not by legal means.

4. What acts are regulated (EU: processing)?

All kinds of data processing, whether by automatic or manual means, are subject to the DSG provisions. Data processing is any operation or set of operations which is performed on personal data, such as collecting, recording, saving, storing, organising, comparing, disclosing, using, erasing and so on.

However, processing by manual means is only subject to the DSG if the data is collected in a data file, that is, a structured collection of data organised by certain criteria. The provisions for manual processing are less strict than for the processing of data by automatic means.

The provisions vary depending on the kind of processing performed. There are special provisions in respect to data transmission (a sub-classification of processing), and there are two types of data transmission defined in the DSG:

- *Überlassung* (mandate transmission), which is the transmission of data from a controller to a processor.
- *Übermittlung* (data transfer), which is transmission from a controller to another recipient who is not a processor.

A processor is defined as a person who has been mandated by the controller to process the data for a specific job on behalf of the controller. The controller is a person who alone or jointly with others determines the purposes and means of the processing of personal data.

5. What is the jurisdictional scope of the rules?

The DSG provisions apply to every kind of processing of personal data in Austria irrespective of the nationality or the origin of the person carrying out the processing. However, in two cases deviating rules apply:

- If data is processed outside of Austria (but in the EU) on behalf of an Austrian establishment of the controller, the DSG applies.
- If data is processed in Austria on behalf of a controller in an EU member state outside Austria, the provisions of that country apply instead of the DSG, unless the purpose of the processing can be attributed to an Austrian establishment of that controller.

The mere "transportation" of personal data through Austria is not subject to the DSG.

6. What are the main exemptions (if any)?

The DSG provides for special exemptions in relation to:

- Private purposes.

- Scientific research and statistics.
- Journalism.
- Processing in case of emergency.

According to these provisions, natural persons can process personal data for private or family purposes if such data was disclosed by the data subject, or if such data has been legally obtained otherwise. Further, the Austrian data protection authority (*Datenschutzkommission, DSK*) (*see box, The regulatory authority*) can give special permission to process personal data for the purpose of scientific research or statistics:

- If obtaining the data subject's consent is impossible or would require disproportional effort.
- If such processing is justified by grounds of public interest.
- If the applicant has credibly shown his expertise.

In relation to journalism the provisions of the DSG apply only partly. The processing of personal data for the purpose of journalism, as defined in the Media Act (*Mediengesetz*), is admissible if and to the extent such processing is necessary for reporting requirements of news agencies, media services and their employees within the fundamental right to free expression of opinion. If there is an emergency, controllers of the public sector and relief organisations can process personal data to the extent necessary to provide help for directly affected persons, to find and identify missing and deceased persons and to provide information for relatives.

7. Is notification or registration required before processing data? If so, please provide brief details.

In general, the DSK must be notified of every data transfer. However, there are several exemptions.

Notification is not required in relation to the data transfer:

- Of published data.
- Of data necessary for public registers.
- Of anonymous data.
- By private persons for private purposes.
- Required for certain media purposes.
- Required for certain state security measures.
- That constitutes a standard process as defined in the Standard and Sample Regulation (*Standard- und Musterverordnung*). Such standard processes include, for example, the data transfer of human resource data for human resources purposes, or the membership administration of private entities.

In general, the data transfer can be carried out as soon as the notification has been filed. The DSK can then advise the controller to amend the notification within two months after the day of notification. After this time has elapsed the notification is final.

However, prior approval by the DSK is necessary if the data transfer:

- Includes sensitive data.
- Includes data about a person's criminal record.
- Is carried out to get information about the data subject's credit standing.
- Is carried out by means of a joint information system (*Informationsverbundsystem*). In a joint information system several controllers have access to a program in which data is processed by all controllers.

Within two months the DSK must decide whether the data transfer can be carried out.

MAIN DATA PROTECTION RULES AND PRINCIPLES

8. What are the main obligations imposed on data controllers to ensure that data is processed properly?

The processing of personal data is only allowed if:

- The purpose and the content of the processing are covered by the legal or contractual authority of the controller.
- In case of data transfer, the recipient has proved his competence in relation to the purpose of the processing.
- The legitimate interest of the data subject in the secrecy of the data is not infringed.
- The constitutional rights of the data subject have not been strained excessively and certain basic principles have been observed.

The basic principles to be observed include:

- Processing in good faith.
- Determining the (legitimate) purpose of the processing, and not processing beyond this purpose.
- Correct entry of the data.
- Only saving the data until the purpose of the processing has been achieved.

9. Is the consent of data subjects required before processing personal data? If so:

- **What rules are there regarding the form and content of consent? Would online consent suffice?**
- **Are there any special rules regarding the giving of consent by minors?**

In some cases the consent of the data subject is required to ensure that his interest in the secrecy of the data is not infringed (*see*

Question 8). However, there are certain circumstances in which consent is not necessary for legal processing (*see Question 10*).

There are very few formal requirements for the consent. If the processing contains sensitive data consent must be given explicitly. The DSG does not require consent to be given in writing, however it is advisable to obtain written consent declarations for evidential purposes. Certain formal standards of consent declarations have been developed based on various court rulings, for example, the wording of the consent declaration must be separate from the rest of the text, it must be clearly readable and it must be signed separately.

However, there are strict rules in the DSG in relation to the content of the consent. Consent is defined as the valid declaration of intention by the data subject to agree to the processing of the data. The data subject must be fully aware of the circumstances, the kind and extent of the processing of the data and must be free of constraint. Such consent can be withdrawn at any time. Therefore, the consent declaration must name each type of data to be processed, the name of the recipients and the exact purpose of the processing. There must also be an indication that the consent can be withdrawn at any time.

There are no special rules regarding minors in the DSG. However, the consent requires a valid declaration of intention, which can only be made by a person of full legal capacity. Since minors do not have full legal capacity they cannot give valid consent to process their data.

10. If there is no consent, on what other grounds (if any) can processing be justified?

The DSG provides three grounds (beside consent (*see Question 9*)) on which processing can be justified:

- The law explicitly states an authorisation or a duty for the processing.
- The data subject has a vital interest in the processing.
- The interest in the processing of the person processing the data or of a third party outweighs the data subject's interest in the secrecy of the data.

There is no definition of the circumstances in which the interest of the controller or a third party outweighs the data subject's interest in the secrecy of the data, but there is a wide spectrum of court rulings which can be used to interpret the provision.

11. Do special rules apply in the case of certain types of personal data, for example sensitive data? If so, please provide brief details.

The processing of sensitive data (*see Question 3*) is subject to stricter restrictions. In many cases, if sensitive data is processed the consent of the data subject is required. Only in special cases consent is not required, such as, if:

- The data has been published by the data subject.
- The identity of the data subject cannot be retraced by legal means (indirect data, *see below*).
- Legal provisions require the processing.
- The data is processed by a public entity within the framework of its duties.
- Only data about a public function of the data subject is processed.
- The processing is necessary to protect vital interests of the data subject and the consent cannot be obtained in time.
- Vital interests of a third party justify the processing.
- The data processing is necessary to enforce a claim.
- The data processing is carried out for private, certain scientific, emergency or medical purposes only. Additionally, certain associations can process sensitive data for specific purposes.

Sensitive data can only be processed after a preliminary check by the DSK. Such processing can be checked by the DSK at any time even without a special cause.

Further, there are special rules in respect to indirect data (*see Question 3*). The legitimate interest of the data subject in the secrecy of the data is not infringed when processing indirect data. There is also no requirement for notification of indirect data.

There are further special provisions for certain types of data in particular cases. For example, the processing of data concerning the criminal record or the credit standing of a person also requires prior approval by the DSK before initiation. There are also special provisions in relation to data processing in the public domain.

RIGHTS OF INDIVIDUALS

12. What information should be provided to data subjects at the point of collection of the personal data?

The minimum information to be provided to the data subject by the data controller at the point of collection of the personal data is the purpose of the processing for which the data is collected and the name and address of the controller. If the data subject is already aware of this information there is no such obligation.

Further information must be provided if processing in good faith requires it. It is definitely required if:

- The data subject has a right to object (*see Question 13*).
- The data subject is not able to recognise whether he is legally obligated to answer the questions asked.
- The data is to be processed in a joint information system (*see Question 7*) which is not based on a legal obligation.

If the data is transferred within the controller's business or from a different controller rather than collected by questioning the data subject, in certain cases the controller has no obligation to inform the data subjects about the data transfer. This exception applies:

- If the processing is required by law.

- If the data subject cannot be reached.
- If the infringement of the rights of the data subjects is very unlikely and the costs of the procedure to inform all data subjects are excessively high.

Finally, there is no obligation to inform the data subject in case the processing is not subject to the duty of notification (*see Question 7*).

13. What other specific rights (such as a right of access to personal data or the right to object to processing) are granted to data subjects?

Data subjects have a right to:

- Information about the personal data concerning them.
- The correction of inaccurate data or deletion.
- Object to the processing.

Right of information

If the data subject asks for information about the data concerning him, the controller must provide information on:

- The data processed.
- The data source, if available.
- The name of all recipients of data transmissions.
- The purpose of the data processing.
- The legal basis for the data processing.

The request for information must be made in writing, unless the controller agrees to oral requests. The data subject requesting information must provide evidence of his identity. The information request can be declined if this is necessary for the data subject's protection, or if there are outweighing legal interests of the controller or a third party.

The controller must provide the information within eight weeks. If the controller declines the information request he must provide reasons for this within eight weeks.

In general, the information is free. If the information is requested in relation to data from a terminated data processing, or if the data subject has already asked for information within the same calendar year, the controller can ask for cost reimbursement.

Right to correction or deletion

Every controller must correct or delete inaccurate and illegally processed data as soon as the inaccuracy or the inadmissibility of the data processing becomes known to him, or if the data subject makes a founded request to do so. The correction or deletion must be effected within eight weeks. If the request of the data subject to correct or delete the data is dismissed the controller must inform the data subject within eight weeks of the reasons for the dismissal.

Right of objection

Every data subject has the right to raise objections to the processing of data concerning him if:

- The processing is not based on a legal obligation.
- The outweighing legal interest in the secrecy of the data resulting from his special situation is infringed on.

If these conditions are met, the controller must delete the data within eight weeks and must refrain from any transfer of this data.

SECURITY REQUIREMENTS

14. What security requirements are imposed in relation to personal data?

Every controller and processor must take measures to ensure data protection. The type and extent of measures to be taken depend on the type of data processed, the amount and purpose of the processing, as well as the technical possibilities and economic viability. The measures must prevent accidental or illegal destruction of the data. They must also ensure proper processing, and that the data is only accessible to authorised persons.

The following security measures should be taken to the extent necessary to ensure the above principles:

- Explicit assignment of tasks to each organisational unit.
- Allow data processing only on valid instructions by authorised personnel.
- Instruct all employees about their duty to provide the necessary data security.
- Regulate the access authorisation to the premises of the data controller or the data processor.
- Regulate the access authorisation to data and computer programs and protect data processing mediums from access by unauthorised persons.
- Define access authorisation to run data processing mediums and install access restrictions to ensure that unauthorised persons cannot access the programs.
- Keep records of the actual processing operations carried out.
- Document all the security measures taken.

PROCESSING BY THIRD PARTIES

15. What additional requirements (if any) apply where a third party processes the data on behalf of the data controller?

The controller may only mandate processors if they are able to ensure legal and secure processing. The controller must settle the necessary details with the processor and check on the processor's compliance by gathering the relevant information.

There are certain duties processors must observe when processing data for the controller (in addition to any contractual duties). Processors must:

- Process the data only within the scope of the agreement.
- Ensure that all necessary security measures are taken (*see Question 14*).
- Only engage other (sub-) processors with the consent of the controller.
- As far as reasonable, provide technical and organisational prerequisites to enable the controller to fulfil his duties in relation to the data subject's right of information, right to correction or deletion, and right of objection (*see Question 13*).
- Return all documents which contain personal data to the processor, or save or delete such documents on behalf of the controller as soon as the processing services have been completed.
- Provide the controller with the information necessary to supervise the duties above.

If data is transmitted to processors outside Austria, or if the controller and processor define the content of these duties in more detail in a contract, this contract must be concluded in writing. Otherwise, the agreement between controller and processor regarding the security measures to be taken does not have to be in writing.

INTERNATIONAL TRANSFER OF DATA

16. What rules govern the transfer of data outside your jurisdiction?

Data transmissions to recipients outside Austria are admissible if the data processing is admissible within Austria (*for requirements, see Question 8*). In addition, in the case of mandate transmissions (*see Question 4*) to recipients outside Austria, the recipient (processor) must agree in writing to observe the general duties of a processor (*see Question 15*) unless the processing is based on certain legal obligations.

Data transfers as well as mandate transmissions to a recipient outside Austria are, in general, subject to the permission of the DSK. There is a general exception in relation to transmissions to a member state of the EU, to Switzerland, Argentina, Canada, Guernsey, Isle of Man, and to recipients in the US who have certified to the US Department of Commerce that they will adhere to the Safe Harbour requirements. Further exceptions exist in relation to certain particular cases, for example, published or indirect data (*see Question 11*) and in respect to data processing which constitutes a standard process as defined in the Standard and Sample Regulation (*see Question 7*).

Permission must be granted if an adequate level of data protection is provided, or if the controller certifies that the legitimate interest of the data subjects in the secrecy of their data will be protected outside Austria. Such certification can be based on contractual warranties.

THE REGULATORY AUTHORITY

Austrian Data Protection Commission (*Österreichische Datenschutzkommission*)

W *www.dsk.gv.at*

Main areas of responsibility. Survey and enforce compliance with the data protection laws, and maintain the data protection register.

17. Are data transfer agreements contemplated or in use? Have any standard forms or precedents been approved by national authorities?

The Austrian legislator has not released or officially approved any standard contractual clauses. However, the standard contractual clauses as defined by the EU (*Commission Decision C(2001)4540, Commission Decision C(2001)1539, Commission Decision C(2004)5271*) are generally accepted by the DSK as sufficient evidence that the standard level of data protection is safeguarded.

18. Is a data transfer agreement sufficient to legitimise transfer, or must additional requirements (such as the need to obtain consent) be satisfied?

Data transfer agreements are sufficient to ensure that the standard level of data protection is safeguarded. However, this is merely one aspect of the legitimacy of data processing. The other conditions (*see Question 8*) must be fulfilled as well, and one requirement might be the consent of the data subject (*see Question 9*). The DSK will only give its permission to transfer data to recipients outside Austria if all conditions for the legitimate processing of personal data are met.

19. Does the relevant national regulator need to approve the data transfer agreement? If so, please provide brief details.

If data is transmitted to a recipient outside the EU the data processing, including the data transfer agreement, needs to be approved by the DSK (*see Question 16*). If the EU standard contractual clauses are used the DSK is compelled to accept them.

The proceedings to receive permission for the data transmission (permission proceedings) are initiated by an application to the DSK. There are no formal requirements for the application. To enable the DSK to evaluate the application, the applicant must specify:

- The type of data to be transmitted.
- The purpose of the processing.
- The names of the recipients.
- The countries of the recipients.

The application for permission is independent of the notification process.

ENFORCEMENT AND SANCTIONS

20. What are the enforcement powers of the national regulator?

Anyone can file a complaint with the DSK about an alleged infringement of data protections rights. There is no charge to file a complaint, and there are no formal requirements.

In case of substantial evidence of an infringement of data protection rights, the DSK can check the data processing complained about. The DSK can ask the controller or processor for information and examine the relevant documents. Data processing which is subject to prior approval (*see Question 7*) can be checked by the DSK even without substantial evidence. The DSK is allowed to enter the premises of the data controller or processor, use the data processing equipment, carry out the processing procedure, and make copies of all relevant documents. The controller/processor is obligated to cooperate with and support the DSK in its investigations.

Further, the DSK can make recommendations to the controller/processor and can set a time limit for the controller/processor to comply with these recommendations. If the controller/processor does not comply within the time limit the DSK can:

- Initiate proceedings to check the registration, which may result in the cancellation of the registration.
- File a criminal complaint, if criminal provisions are applicable.
- If the data subject is a private (natural or legal) person, file an action for a declaratory judgment against the controller/processor before civil courts.
- If the data subject is a public entity, inform the competent supervisory authority.

The DSK is competent to rule on a complaint regarding an infringement of the right of information (*see Question 13*). In relation to complaints regarding an infringement of the right to correction or deletion, the DSK is only competent if the controller/processor is a public entity (except legislative or judicial bodies). For all other cases the DSK is not competent; the claims must be filed with the civil courts instead.

21. What are the sanctions and remedies for non-compliance with the data protection laws? To what extent are the laws actively enforced?

In cases of infringement of the right of data protection or the right to correction or deletion, the data subject can claim for an injunction and cessation of the infringement. The court can grant an interim injunction in this regard. Such claims must be brought before the civil courts.

Further, the data subject can file an action for damages with the civil courts. The prerequisite for indemnification is the existence of a financial loss, caused by the infringement of data protection regulations, based on negligent conduct.

The controller and processor are liable for the actions of their personnel. They can be discharged from liability if they can prove that neither they nor any of their personnel are liable for the infringement.

The Crimes Act (*Strafgesetzbuch*) contains several provisions which might apply in cases of data protection infringement. For example, the illegal access to a computer system, the abusive trapping of electronic data as well as manipulation of an electronic processing with the intention of unjustified enrichment are prohibited. The penalty is a pecuniary fine or up to six months imprisonment.

The DSG also contains criminal sanctions. The wilful infringement of data protection with the intention of unjustified enrichment or to harm another person is prohibited under penalty of up to one year imprisonment.

Further, the DSG contains administrative penalties of up to EUR18,890 (about US$24,000) for:

- Wilful illegal data access.
- Wilful illegal data transfer.
- Illegal processing despite a binding court ruling.
- Wilful deletion of data despite a request for information.

A penalty of up to EUR9,445 (about US$12,000) applies for cases in which:

- The duty of notification is violated.
- Data is transmitted to a recipient outside Austria without the permission of the DSK.
- A data controller does not comply with its duties to inform the data subjects or the DSK.
- If the necessary security measures have not been taken.

Finally, an infringement of data protection laws might give rise to claims based on competition law.

CONTRIBUTOR DETAILS

Dr Ferdinand Graf
Graf & Pitkowitz Rechtsanwälte GmbH
T +43 1 401 17 0
F +43 1 401 17 40
E *graf@gmp.at*
W *www.gmp.at*

Areas of practice/expertise. Dr Ferdinand Graf is admitted to practise in both Austria (1993) and New York (1994). He is a founding partner of Graf & Pitkowitz Rechtsanwälte GmbH. Dr Graf is head of the firm's competition and IP/IT department. He is a member of the Vienna Bar Association, and also the American, New York State and the International Bar Association.