International Transfers of Personal Data
Treatment of Personal Data Transfers in Europe
Austria

Rainer Knyrim*

1. Introduction

Austria is a member of the European Union (EU) and has therefore implemented the EU Directive 95/46 on the Protection of Individuals with regard to the Processing of Personal Data (the Directive).

The Directive has been implemented by the Austrian Data Protection Act 2000 (ADPA),[1] which applies to all processing of personal data by automatic means. In addition, the nine Austrian states (Bundesländer) have adopted data protection laws, which apply to processing of personal data by means other than automatically.

Section 1 para. 1 ADPA, which has a constitutional status, states that everybody shall have the right to secrecy of the personal data concerning them, especially with regard to their private and family life, insofar as they have an interest in 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. That means that personal data cannot be used, unless there is a special justification.

According to Section 1 para. 1 ADPA, the provisions of the ADPA apply to the use of personal data in Austria. Additionally, the ADPA applies to the use of data outside of Austria, insofar as data are used in other member states of the EU for purposes of the controller's main establishment or branch establishment in Austria.

There is a new draft law for a Data Protection Act 2010, which introduces several changes, in particular regarding video images and the filing process. There are no changes envisioned regarding data transfers and data transmissions.[2]

2. Personal Data

2.1. Definitions

- **Data** (personal data) is information relating to data subjects who are identified or identifiable; data are "only indirectly personal" for a data controller, a processor or recipient of a transfer when the data relate to the data subject in such manner that the controller, processor or recipient of a transfer cannot establish the identity of the data subject by legal means.[3] The Austrian Data Protection Commission (ADPC) considers for example phone numbers as the subscriber's personal data as the subscriber is identifiable by the phone number or a reference number.[4]
- **Sensitive data** (data deserving special protection) are defined as 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.[5]
- Unlike other member states of the EU, a data subject is defined as any natural or legal person or group of natural persons not identical with the data controller, whose data are processed. This means that also legal persons can be data subjects and have—with minor differences—the same rights as natural persons.[6]
- A data controller is a natural or legal person, a group of persons or organ of a territorial corporate body or the offices of these organs, if they decide alone or jointly with others to process personal data for a specific purpose, without regard whether they process the data themselves or have the processing carried out by somebody else. The above-mentioned persons, groups of persons or institutions are also deemed to be controllers when they give personal data to somebody else for a commissioned work and that person decides to process the personal data for its own purposes. If the contractor was expressly prohibited from processing the data for its own purposes when commissioned or if the contractor himself decides on the use, in particular whether to process the personal data for its own purposes, pursuant to legal provisions, professional rules or codes of conduct, the contractor is regarded as a data controller itself.[7]
- A data processor is a natural or legal person, a group of persons or an organ of a federal state and local authority or the offices of these organs, who process data that were given to them for a commissioned work on behalf of the data controller.[8]

2.2. Conditions for the Processing of Personal Data

2.2.1. Non-sensitive personal data may be processed if one of the following conditions is fulfilled:[9]

a) Legal authorization: According to an explicit statutory basis the controller has the right to process data; or

b) Consent: The data subject has given his consent to the data processing, which can be revoked at any time. The revocation makes any further use of the data illegal. The Austrian Supreme Court (the "Court") and the ADPC have placed very strict conditions for a legally correct consent form. The consent form has to mention every processed (or in case of a transfer, every transferred) data type, as well as the corresponding processing purpose. In case of a data transfer every data recipient and the purpose for the transfer as well as the information about the possible revocation have to be mentioned also. The Court is of the opinion that an employee cannot give a free consent during an existing employment contract as the employee is always pressured by the employer; or

c) Vital interests: The use of the data can be necessary for the data subject's vital interests; or

d) Legitimate interests: The data processing is also allowed if the controller's or a third party's prevailing interests require the use of data. In this sense the data subject's interests are not infringed if the use of non-sensitive data:

- Is an essential requirement for a controller in the public sector to exercise a legally assigned function or
- Is performed by a controller of the public sector in fulfillment of his obligation to provide inter-authority assistance or
- Is required to protect the vital interests of a third party or
- Is necessary for the fulfillment of a contract between the controller and the data subject or
- Is necessary for establishment, exercise or defense of legal claims of the controller before a public authority and if the data was collected legitimately or
- Concerns solely the exercise of a public office by the data subject or
- In case of a catastrophe, to the extent required to assist the persons directly affected by the catastrophe, to locate and identify persons missing or dead and to inform relatives; or

e) Published data: If data, which have already been permissibly published, are processed, no legitimate interests are infringed.

A data controller is only allowed to use data if one of the preceding conditions is fulfilled.

2.2.2. Sensitive data may solely be processed if one of the following conditions is fulfilled:[10]

a) Public data:[11] The use of sensitive data is allowed if the data subject has made public the data himself; or

b) Indirectly personal:[12] The use is also permitted if the used data are only indirectly personal; or

c) Legal basis:[13] Another possible condition is a right or obligation based on a legal rule, insofar as such rule serves an important public interest; or

d) Obligatory administrative assistance:[14] The use is allowed if the data are used by a controller in the governmental domain in performing obligatory administrative assistance; or

e) Public office:[15] The used data only affect the data subject's exercise of a public office.

f) Clear consent:[16] The data subject has given his/her clear consent, which can be revoked at any time and without any reason and makes any further use of the data illegal. Please note that the Austrian Supreme Court and the ADPC have placed very strict requirements for a valid consent form (point 2.2.1 b). The difference to the processing of non-sensitive data is that in case of the processing of sensitive data the data subject has to give his/her clear consent (an implied consent is not enough).

g) Data subject's vital interest:[17] The processing or data transfer is in the data subject's vital interests and his/her consent cannot be obtained in time; or

h) Third party's vital interest:[18] The use of the data is in a third party's vital interest; or

i) Legal claim:[19] The use is necessary for the establishment, exercise or defense of legal claims before a public authority (this includes amicable arrangements before the commencement of a trial); or

j) Research:[20] Data are used for scientific research or statistics; or

k) Employer obligations:[21] The employer needs to use the data to fulfill its obligations as an employer; or

l) Medical data:[22] The use of data is required for purposes of

preventive medicine, medical diagnosis, the provision of health care or treatment or the management of health-care services and is used by health care professionals; or

m) Non-profit organizations:[23] Non-profit-organizations 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 the data relate to the members, sponsors or other persons who display an interest in the aim of the organization on a regular basis; the data shall not be disclosed to a third party without the data subject's consent, unless otherwise provided by law.

The legal basis for the use of sensitive data is mostly identical with Art 8 para 2 and 3 of the Directive; the Austrian legislative body added some additional requirements. The most important justifications are the existence of a legal basis, a clear consent and the employer's obligations.

3. Data Transfer

3.1. General

Data transfer is the transfer of data contained in a data "application" to recipients other than the data subject, the controller or processor, in particular the publishing of such data as well as the use of data for the controller's other purposes.[24] It does not make any difference if the data are actually transferred to a third person or if the third person gets access to the data at the controller's place. Also the transfer from one of the data controller's departments to another one (for another purpose) is seen as a data transfer, as data are only allowed to be used for distinct purposes. A department is seen as one of the controller's fields of activity, which form a part of the controller's whole business.

Data may only be transferred, if they come from a permitted data application, if the receiver has made plausible his/her legal competence and the transfer does not infringe the data subject's interest of secrecy.[25]

3.2. Obligation to Disclose the Controller's Identity

A data controller has the obligation to disclose his/her identity in an appropriate manner in case of data transfers and communication to the data subject.[26] This duty helps the data subject to exercise his/her rights (such as the right to revoke the given consent or the data processing or transfer or to deletion).

If the controller violates this obligation, s/he commits a breach of administrative law and can be compelled to pay up to EUR 9445.00.[27]

3.3. Requirements for a Data Transfer outside of Austria

Generally, data are only allowed to be transferred or transmitted outside of Austria, if the data application is lawful in Austria.[28] Additionally the data recipient has to prove his/her legal competency to receive and process the data. The data transfer or transmission would have to be allowed if the recipients are within Austria. In case of data transmissions to foreign countries the foreign data recipient has to ensure that s/he fulfills the Austrian obligations according to Section 11 ADPA in written form.

Basically the data transfer and data transmission to another member state of the EU is not subject to any special restrictions[29] (as mentioned in Section 13 ADPA). This is part of the Directive's harmonization of an adequate data protection level. If the Directive is not applicable, the transfer needs a prior authorization.

If the data are transferred to third countries with an adequate data protection level, no permission is needed, either.[30] According to the European Commission's conclusion about the adequacy of the data protection levels in third countries, for example Switzerland has an adequate level of data protection. Controllers or providers in the USA have an adequate level of data protection if they are Safe Harbor certified. Such a level can also be established by signing the EU Standard Contractual Clauses.

In addition there are some other exceptions, where no permission is needed, for example if the data subject has given his/her consent[31] or if the data has been permissibly published in Austria.[32] In all other cases a data transfer to third countries requires the ADPC's prior permission.

Generally, data applications have to be notified with the Austrian Data Processing Register (the "Register"). The federal chancellor released the decree on the Standard and Model Applications.[33] If no more data types than described in the model applications are processed and no more data transfers take place, the controller only has to file the model application, which will be registered. In case of standard applications, the application does not have to be filed at all. If one data type or one transfer to another data receiver happens, the whole data application has to be filed.

The most important legal bases for a data transfer or a data transmission to third countries are described below.

3.3.1. Safe Harbor Certification for Data Controllers from the USA

The Directive prohibits the transfer of personal data to non-European Union countries that do not meet the European "adequacy" standard for privacy protection. The privacy standards between the

USA and the member states of the European Union differ; the US privacy protection standards are presumed as being lower, which means that without any special rules no data could be transferred between the European Union and the USA without prior permission.

In order to bridge these different privacy approaches and provide a streamlined means for US organizations to comply with the Directive, the US Department of Commerce, in consultation with the European Commission, developed a so called "Safe Harbor" framework. Entities that want to be Safe Harbor certified have to accept the so-called Safe Harbor Principles and the Frequently Asked Questions.

In 2000 the European Commission accepted that US companies that are Safe Harbor certified have an adequate data protection level.[34]

There is a list of all Safe Harbor certified entities on the Internet.[35] This list should be checked, whenever a data transfer between an entity of the USA and an entity of the EU takes place.

3.3.2. Consent

The data transfer to third countries does not require permission if the data subject has undoubtedly given his/her free consent to the data transfer or transmission into the third country. Only people who are contractually capable can effectively consent to a data transfer. This excludes children younger than seven years and people with decreased mental capabilities. Furthermore, the consent has to be given freely, seriously, decisively and comprehensibly.

To fulfill the aforesaid, the data subject has to be informed about the transferred or transmitted data types (exhaustive listing), the purpose of the data transfer and the data recipients as well as about the country in which the data recipients are located.[36] Only if the data subject possesses all this information can s/he actually consent. The data recipients can either all be mentioned in the consent form or there can be a link to a website, where all data recipients are listed (e.g. in case of the members of an affiliated group). The main condition for an effective consent is that the data subject is informed about the conditions and that s/he understands them.

The ADPA does not set any special requirements for an effective consent. Therefore consent can be given orally or written or even on the Internet by ticking a "yes"-box. In case of the data processing of sensitive data the consent has to be given specifically, which excludes implied consents. Such specifically given consent cannot just be part of a company's general terms and conditions, but the data subject has to give his consent apart from any other contractual agreement. This means that the consent form has to be clearly set apart from the rest of the text. In addition the type size of the consent form has to be at least as big as the rest of the text and the consent form has to be

signed separately.[37]

A once given consent can be revoked at any time; the revocation makes any further data transfer illegal. Every consent form has to refer to the data subject's right to revoke the consent. Regarding consumers the Court has stated that the absence of such notice makes such clause non-transparent in the sense of Section 6 para. 3 of the Austrian Consumer Protection Act.[38] Therefore, it is highly recommended to refer to the data subject's right to revoke the consent in every consent form.

Regarding employment, the Austrian courts have opined that consent cannot be given freely, because of the employer's pressure on the employee. Therefore in such cases a popular legal base for the data transfer (and processing) would be the contractual necessity (see point 3.3.3) of the processing and transferring.

3.3.3. Contractual Necessity[39]

A transborder data transfer to third countries is also allowed if the data transfer is necessary to fulfill a contract between the data controller and the data subject or between the data subject and a third person in favor of the data subject. For example a travel agency would have to disclose the traveler's data to the airline in order to get the flight ticket for the traveler.

The reference to the contractual necessity is only possible regarding nonsensitive data, because this legal basis is not mentioned regarding sensitive data in Section 9 ADPA. Thus, even though the transfer of the sensitive data is necessary to fulfill a contract, it is only possible with the data subject's consent or another enumerated basis under Section 9 ADPA.

In connection with employment contracts, it is seen that data processing or data transfer is mostly not covered by the employee's consent, but rather by the contractual necessity of the processing or of the transfer.

3.3.4. Important Public Interest or Vital Interest of the Data Subject[40]

According to Section 12 para. 4 ADPA data can be transferred or transmitted to third countries if the data transfer is necessary for upholding an important public interest or the data subject's vital interest and the transfer or transmission is so urgent that the ADPC's permission cannot be obtained prior to the transfer without placing this interest in peril. In this case the ADPC has to be informed about the transfer or transmission immediately.

3.3.5. Necessity for the Assertion of Legal Claims[41]

The data controller is authorized to transfer or transmit data to

third countries if this transfer or transmission is necessary to assert, exercise or defend legal claims.

3.3.6. The EU Commission's Standard Contractual Clauses[42]

If there is no legal basis according to Section 12 ADPA, permission for the data transfer or data transmission has to be sought from the ADPC.[43] The ADPC is free to put conditions on the transfer or transmission. The transfer is generally allowed and permitted if the third country has an adequate data protection level. Adequacy can also be established by special agreements between the data controller and the recipient of the data, such as the Standard Contractual Clauses of the European Commission.

According to Article 26 of the Directive the EU Commission has the right to create so called Standard Contractual Clauses, which can be used and signed by the data exporter and the data importer. Based on this foundation the EU Commission has issued three decisions including three different Standard Contractual Clauses. If the parties utilize those Standard Contractual Clauses, they nevertheless have to get the Data Protection Commission's permission for the transfer. The relief is that in case the signed and filed clauses are not different from the original ones, the ADPC will not discuss the content of the Clauses, but only the Appendices thereof.

3.3.7. Procedure

The procedure with the ADPC for the approval of an international data transfer starts with a written application letter, which is typically accompanied with signed EU Standard Contractual Clauses. Usually the ADPC asks questions regarding the application letter. The approval procedure will usually take several months and costs about 30 Euros.

3.3.8. Binding Corporate Rules

Another possibility to get the ADPC's permission for the data transfer or data transmission to third countries according to Section 13 ADPA is that affiliated companies conclude the so-called Binding Corporate Rules. This is a self-commitment to keep certain data protection rules as specified in the Rules. The benefit is that not every change within the data applications results in a new permission procedure with the ADPC. The disadvantage on the other hand is that it takes relative long to work out the Rules and have them approved by all concerned local DPA's.

4. Regulatory Filing with the Data Processing Register

4.1. Notification of Data Applications

A data controller is obliged to notify every data application, which

contains personal data with the Austrian Data Processing Register (the Register) unless it falls under an exemption listed in the Standard and Model Applications Ordinance.[44] An exemption is made for relatively simple and frequently occurring data applications, such as customer data, including the use of data for marketing purposes.

If a data application falls under a standard application, it does not have to be filed with the Register. The problem is that in most cases the data transfers—especially to the parent company—are not covered by the standard applications. Therefore, a notification with the Register has to be made for the underlying data processing done in Austria.

4.2. Special Forms for Notification of Data Applications

There are special forms for a notification of data applications.[45] These forms can be sent to the Register by email. Normally the data processing can be commenced immediately after the filing.

Certain data applications can only be initiated after a prior check of the notification by the Register resulted in a positive outcome. The applications that require prior checking by the Register are detailed in Section 18 Para 2 ADPA. All other data applications may be initiated immediately after the notification has been submitted to the Register.

If an approval for international data transfer is necessary due to the lack of the data subject's consent, such an approval needs to be applied for by letter to the ADPC (in parallel to the notification with the Register).

4.3. Controller Files Application

Basically, the controller has to file a notification, the conditions of which are laid down in Section 19 ADPA, with the Register. The duty to notify also applies to all circumstances that subsequently lead to the incorrectness or incompleteness of the notification. This means that a data controller has to check the up-to-datedness of the filed data from time to time and amend it, where necessary.

The Register shall examine a notification within two months. If the Register comes to the conclusion that the notification is insufficient in terms of Section 19 Para 3 ADPA, the controller shall be ordered within two months after receipt of the notification to correct the insufficiency within a certain period (normally 4 weeks). It is very common that a correction order is received on the last days of this two months delay, because this gives the Register time to check the notification beyond the two months period. If the order is not complied within a timely manner, the Register can refuse registration; otherwise the notification shall be regarded as if it had been correct from the beginning. If no order for correction is made within two months after the notification, the Register considers the obligation to notify as fulfilled. Data applications subject to prior checking pursue to Section

18 Para. 2 ADPA may then be commenced. The notification procedure typically lasts several months, because of the correction order. It does not cost anything.

4.4. Notification Before Commencement

As mentioned above, the data processing has to be notified before it is commenced, except for standard applications, which do not have to be notified.[46]

4.5. Content of Notification

Notifications must contain the data controller's name (or other destination) and address also of his representative; furthermore the controller's registration number, insofar one has already been assigned to him, and the proof of statutory competence all of the legitimate authority that the controller's activities are permitted, if so required and the purpose of the data application to be registered and the legal basis, the categories of data subjects and the categories of data about them that are processed and the categories of data subjects affected by intended transmissions, the categories of data to be transmitted and the matching categories of recipients—including possible recipient states abroad—as well as the legal basis for the transmission and—insofar as a permit by the ADPC is required—the file number of the permit of the ADPC as well as a general description of data security measures taken pursuant to Section 14, which enable a preliminary assessment of the appropriateness of the security measures. Application for international data transfers will require similar details.

4.6. Detailed Information

The Austrian Data Protection Authorities are probably some of the strictest in the world with regard to requesting very detailed information on data fields, recipients and purposes of the processing/transfer and will not grant any notification or permission, if their information requests have not been entirely satisfied. Therefore it is advised to keep close contact with the Register and/or the ADPC.

5. Consequences of Noncompliance

According to Section 52 para. 2 ADPA an administrative offence punishable by a fine of up to 9445.00 Euro is committed by anyone who collects, processes and transmits data without having fulfilled his obligation to notify according to Section 17 or engages in transborder data transfer or transmission without the necessary permit of the ADPC according to Section 13—insofar as the committed act does not fulfill the legal elements of a criminal offence subject to the jurisdiction of the courts of law.[47]

NOTES:

[1]Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 – DSG 2000) (NR: GP XX RV 1613 AB 2028 S. 179. BR: 5992 AB 6034 S. 657.) (CELEX-Nr.: 395L0046) StF: BGBl. I Nr. 165/1999 = Federal Act concerning the Protection of Personal Data.

[2]62/ME (XIV. GP); GZ 810.026/0005-V/3/2009; Bundesgesetz, mit dem das Bundes-Verfassungsgesetz das Datenschutzgesetz 2000 und das Sicherheitspolizeigesetz geändert werden, (DSG-Novelle 2010); http://www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00062/pmh.shtml.

[3]§ 4 lit 1 ADPA.

[4]Eg, ADPC November 12, 2004, K120.896/0018-DSK/2004.

[5]§ 4 lit 2 ADPA.

[6]§ 4 lit 3 ADPA.

[7]§ 4 lit 4 ADPA.

[8]§ 4 lit 5 ADPA.

[9]§ 8 ADPA.

[10]§ 9 ADPA.

[11]§ 9 lit 1 ADPA.

[12]§ 9 lit 2 ADPA.

[13]§ 9 lit 3 ADPA.

[14]§ 9 lit 4 ADPA.

[15]§ 9 lit 5 ADPA.

[16]§ 9 lit 6 ADPA.

[17]§ 9 lit 7 ADPA.

[18]§ 9 lit 8 ADPA.

[19]§ 9 lit 9 ADPA.

[20]§ 9 lit 10 ADPA.

[21]§ 9 lit 11 ADPA.

[22]§ 9 lit 12 ADPA.

[23]§ 9 lit 13 ADPA.

[24]§ 4 lit 12 ADPA.

[25]§ 7 para. 2 ADPA.

[26]§ 25 ADPA.

[27]§ 52 para. 2 lit 3 ADPA.

[28]§ 12 para 5 ADPA.

[29]§ 12 para. 1 ADPA.

[30]§ 12 para. 2 ADPA.

[31]§ 12 para. 3 lit 5 ADPA.

[32]§ 12 para. 3 and 4 ADPA.

[33]Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV

2004), BGBl. II Nr. 312/2004.

[34]2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (text with EEA relevance); Official Journal L 215, 25/08/2000 P. 0007 – 0047.

[35] www.export.gov/SafeHarbor/.

[36]Austrian Supreme Court, OGH January 27, 1999, 7 Ob 170/98w.

[37]Newsletter from the Federal Chancellery of the Republic of Austria of August 10, 1985, BKA-VD, 810.008/1-V/1 a/85.

[38]OGH 19.11.2002 4 Ob 179/02f; OGH 20.03.2007 4 Ob 221/06p.

[39]§ 12 para. 3 lit 6 ADPA.

[40]§ 12 para 4 ADPA.

[41]§ 12 para. 4 lit 7 ADPA.

[42]EU Commission's decisions 2001/497/EC of June 15, 2001; 2004/915/EC of December 27, 2004; 2002/16/EC of December 27, 2001.

[43]§ 13 para. 1 ADPA.

[44]Verordnung des Bundeskanzlers über Standard- und Musteranwendungen nach dem Datenschutzgesetz 2000 (Standard- und Muster-Verordnung 2004 – StMV 2004), StF: BGBl. II Nr. 312/2004 = Standard and Model Applications Ordinance according to the Data Protection Act.

[45] www.dsk.gv.at/site/6296/default.aspx.

[46]§ 17 para. 1 ADPA.

[47]§ 52 para. 2 lit 1 ADPA.