GETTING THE DEAL THROUGH

Data Protection & Privacy

in 26 jurisdictions worldwide

2014

Contributing editor: Rosemary P Jay

Published by
Getting the Deal Through
in association with:

Adams & Adams

Arzinger

Coelho Ribeiro e Associados

Com advokatbyrå

Drew & Napier LLC

ELIG, Attorneys-at-Law

Gilbert + Tobin

Heenan Blaikie LLP

Hoffmann Liebs Fritsch & Partner

Hunton & Williams LLP

Ichay & Mullenex Avocats

Iriarte & Asociados

Jayaram & Jayaram

Laux Lawyers, Attorneys-at-Law

Lee and Li, Attorneys-at-Law

Lexing Spain

Lorenz International Lawyers

Matheson

MNKS

Nagashima Ohno & Tsunematsu

Olivares & Cia

Panetta & Associati Studio Legale

Pinheiro Neto Advogados

Preslmayr Rechtsanwälte OG

Yoon & Yang LLC

GETTING THE DEAL THROUGH

Data Protection & Privacy 2014

Contributing editor
Rosemary P Jay
Hunton & Williams

Publisher
Gideon Roberton

Business development managers
Alan Lee
George Ingledew
Dan White

Account manager
Megan Friedman

Trainee account managers
Cady Atkinson, Joseph Rush, Dominique Destrée and Emma Chowdhury

Media coordinator
Parween Bains

Administrative coordinator
Sophie Hickey

Trainee research coordinator
Robin Synnot

Marketing manager (subscriptions)
Rachel Nurse
subscriptions@gettingthedealthrough.com

Head of editorial production
Adam Myers

Production coordinator
Lydia Gerges

Senior production editor
Jonathan Cowie

Subeditor
Davet Hyland

Director
Callum Campbell

Managing director
Richard Davey

Data Protection & Privacy 2014
Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2012
Second edition

ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

Law Business Research

CONTENTS

Austria

Rainer Knyrim

Preslmayr Rechtsanwälte OG

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The legislative framework for the protection of personally identifiable information (PII) in Austria mainly consists of the Data Protection Act (ADPA). Besides, privacy-related provisions can be found for example in the Telecommunications Act regarding electronic advertising and the processing of personal communication data of users by telecommunication service providers, in the Act on Banking regarding banking secrecy as well as in the Labour Constitutional Act regarding data applications for purposes of personnel administration and evaluation. In the field of health care the Health Telematics Act 2012 states technical data security measurements to be implemented for the transmission of health data among health service providers and contains provisions for the implementation and operation of the Federal Electronic Health Record.

The ADPA was enacted in 2000 and is the most relevant data protection act in Austria. It implemented the EU Data Protection Directive 95/46/EC (the Directive) and regulates which types of personal data may be processed by whom and under what circumstances and conditions. In addition, it should be noted that the right for the protection of personal data has constitutional status in Austria.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the powers of the authority.

At present, the competent authority is the Data Protection Commission, but from 1 January 2014 it will be transformed to the Data Protection Authority. The Data Protection Authority (DPA) is an independent body and ensures that individual rights and interests in secrecy of personal data is protected. In addition, the DPA handles complaints.

The DPA decides on notifications of data applications, applications for authorisations of data transfers to countries outside the European Economic Area (EEA) as far as those countries do not provide an adequate level of protection and it functions as a complaint authority for anyone whose rights for privacy or data protection have (allegedly) been infringed.

In case of an infringement the DPA is also able to request detailed information from the data controller and processor and then has the power to carry out audits and inspections. Furthermore, the DPA is empowered to report an offence to the department of public prosecution or to file claims with the responsible court in case of severe infringements of data protection law.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

Breaches of data protection regulations can lead to criminal or administrative penalties. Any individuals that – with the intention to make profits or to harm others – use, make available to others or publish personal data entrusted to or made accessible to them solely due to professional reasons or which they acquired illegally, will be punished by court with imprisonment of up to one year, unless the offence is subject to more severe punishment pursuant to another provision.

Anyone committing any of the following may be punished with a fine of up to €25,000:

- intentionally and illegally gains access to a data application or keeps up an obvious illegal access;
- intentionally transmits personal data in violation of the rules on confidentiality and, in particular, misuses data entrusted to him or her pursuant to the provisions granting the use of personal data for scientific research and statistics or of address data to inform or interview data subjects for other purposes;
- uses personal data or fails to grant access to such data to rectify or to erase personal data in violation of a valid judicial or administrative decision;
- intentionally erases personal data in violation of section 26 paragraph 7 ADPA; or
- intentionally acquires personal data in case of disaster under false pretences violating section 48a ADPA.

Anyone who commits any of the below offences may be punished with a fine of up to €10,000:

- collects, processes or transfers personal data without fulfilling his or her notification duty for data applications or video surveillance or operates a data application that deviates from his or her filing;
- transfers personal data abroad without a required prior approval of the Data Protection Authority;
- infringes commitments given to the Data Protection Authority or infringes stipulated constraints;
- infringes his or her disclosure and information duties to data subjects;
- grossly infringes his or her duty to implement appropriate data security measurements pursuant to section 14 ADPA;
- infringes his or her duty not to perform automatic image matching on video surveillance material, not to scan surveillance material for sensitive data automatically or to log the utilisation of surveillance material; or
- infringes his or her duty to delete surveillance material after its legal retention period.

In addition, anyone who fails to grant access to personal data, to rectify or to erase personal data in violation of the ADPA, unless the

offence is subject to more severe punishment pursuant to another provision, may be punished by a fine of up to €500.

Furthermore, the Austrian Criminal Law also contains rules for punishments in case of violations concerning data.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

As a consequence of the constitutional status of the right for the protection of personal data, the data protection law is applicable in all sectors. No type of organisation is exempted. Both public authorities and private organisations have to obey the rules imposed by data protection law.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Since each of these activities regularly leads to the electronic use of personal data, the provisions of the ADPA generally are applicable in these matters. As previously stated, areas such as telecommunication or electronic marketing are regulated in the Telecommunications Act; monitoring employees and appraising their performance is governed by the Labour Constitutional Act which, to the extent of the respective provisions, also forms part of Austrian data protection law. Video surveillance as well as analysing protocol data to assess the behaviour of data subjects is also covered by the ADPA.

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

A specific act exists for the transmission of health data among health service providers and for the Austrian Electronic Health Record, but with respect to the core regulations of data protection, this Act refers to the ADPA. The same is true for regulations on credit information: credit information databases are mentioned in a few acts referring to data protection, which have incorporated general provisions to be applied to various areas connected to the processing of personal data. The E-Government Act provides regulations for a Federal Identity Management to enable authorities to identify people uniquely in governmental proceedings. This act also regards aspects of data protection by defining an identity management system that prevents the possibility of merging personal data across multiple authorities. If smart meters are used for the supply of electricity or gas the applicable acts contain provisions for the protection of personal data and grant customers the right to have their data accessed or transmitted via the internet (Electricity Industry and Organisation Act 2010, Gas Industry Act 2011).

7 PII formats

What forms of PII are covered by the law?

In general, all activities regarding the use of PII are covered by the ADPA, but most provisions, such as the notification duty, are only relevant for the electronic processing of personal data and for the manual processing of personal data in structured records accessible via one specific search criterion. Moreover, the ADPA does not only protect the personal data of natural persons but also of legal persons and groups of persons.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

The ADPA applies to the use of personal data in Austria. The ADPA also applies to the use of data outside Austria insofar as the data is used in other member states of the EU for the purposes of the main establishment or a branch establishment of the data controller in Austria. Apart from this general rule, however, the law of the state in which the data controller has its seat applies where a data controller in the private sector whose seat is in another EU member state uses personal data in Austria for purposes that cannot be attributed to any of the data controller's establishments in Austria. Furthermore, said law shall not be applied insofar as the data is only transmitted through Austrian territory.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

Austrian data protection law gives broad cover to the processing of personal data; any type of processing such as collecting, storing, transferring, viewing, giving access, etc, is covered by its provisions. A very important distinction in practice is made between the transfer of personal data and the mere 'handover' of data to a third party for the sole purpose of the provision of services to the controller. If the receiver of the data uses the data for its own purposes, then data is regarded as having been transferred. In most cases, a transfer of personal data must be notified with the DPA and there are certain underlying restrictions (eg, the transfer has to serve a legitimate purpose of the recipient, a transfer to outside the EEA has to be authorised by the DPA, unless certain exemptions like a Safe Harbor certification in the United States apply).

In general, a commitment of data to a service provider does not have to be notified with the DPA, but the commitment of a service provider established outside Austria must be governed by a written contract between the data controller and the data processor which especially regulates the handling of data by the service provider. Moreover, if the service provider is established outside the EEA, the DPA's authorisation for the committing of the data is necessary, unless one of the exemptions applies as mentioned in question 31.

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent? Give details.

Yes, Austrian data protection law requires a legitimate purpose and a legal basis for each processing and transmission of personal data. Four major possible legal bases are provided by the ADPA:

- processing is required to comply with the law;
- the data subject has given his or her explicit consent;
- processing of data is required for the vital interests of the data subject; and
- the interests of the controller in the processing of data prevail over the legitimate interests of the data subject in the protection of his or her data.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

There are four specific types of data for which more stringent rules are applicable:

- sensitive data (ethnic origin, political opinions, membership in unions, religious or philosophical views, health and sex life);

- data related to criminal convictions;
- data revealing information on the credit status of the data subject; and
- data being part of a joint information system.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

The ADPA obliges data controllers to inform data subjects about the purposes of the data application as well as about the data controller's name and address, as far as this information is not available to the data subject anyway. Further information has to be provided appropriately, as far as necessary for a data processing in good faith, especially if the data subject has the right to object the processing of its data, if it's ambiguous for the data subject whether he or she is legally obliged to provide the requested data or if data is processed within a joint information system.

If the data controller operates a video surveillance system, monitored areas have to be marked with appropriate signs in order to enable individuals to avoid entering observed areas.

13 Exemption from notification

When is notice not required (for example, where to give notice would be disproportionate or would undermine another public interest)?

A data application is exempted from notification once it is completely covered by a 'standard application'. Standard applications are regularly published as a regulation by the Federal Chancellor of Austria and list personal data that may be legitimately processed for designed purposes; in addition, the exemption applies only if the data is transferred to those categories of recipients named in the relevant standard application only.

Furthermore, an application is exempted from notification if:

- only published personal data is processed;
- only pseudonymous personal data is processed, provided that the controller is not able to identify data subjects legitimately but only somebody else;
- the application implements a publicly accessible register or directory established pursuant to a legal provision; or
- the application is operated for private or family purposes only.

Exemptions also exist for data applications serving one of the following purposes:

- protection of the constitutional establishments of the Republic of Austria;
- safeguarding the operational readiness of the Austrian Army;
- safeguarding the interests of a comprehensive national defence;
- protection of important foreign-policy, economic or financial interests of the Republic of Austria or the European Union; or
- prevention and prosecution of crimes, as far as is necessary to meet these purposes.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

The controller of personal data must provide subjects with access to their data. Upon the data subject's request, the controller has to rectify or even erase the data, unless the controller has a legitimate interest regarding the processing of the data.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

As soon as data is collected and stored, the data controller has the obligation to ensure that the data is always correct and kept up to date, as long as their accuracy is necessary to fulfil the intended purposes. In addition, the controller has to ensure that data is only stored as long as is necessary for the legitimate purpose of their processing, and as long as both the purpose and the legal basis for the processing exist with respect to any particular individual that is subject to the application (eg, the individual might withdraw his or her consent, the employee might have left the company, etc).

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

The law restricts the amount of data held by establishing the principles of data minimisation, which means that only those data may be held that are absolutely necessary for the achievement of the purpose for which the data is collected. Similarly, data may only be held for the amount of time necessary for the purpose and as long as required by law (if applicable). Otherwise, data has to be deleted physically, a logical deletion is not sufficient (eg, if the respective data is only marked as being deleted in the database or if only the respective indices in the file system are removed).

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

A purpose limitation principle in the sense that the processing of data is only legitimate for specific purposes has been adopted. The processing of data is allowed for any legitimate and valid purpose.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The purpose has to be evaluated individually for every single case. Often, a balancing of the controller's interests with those of the data subject is necessary and delivers the answer whether the use of personal data is legitimate or not. If personal data shall be used for other purposes a further use has to be treated like a data transmission to other data controllers. Therefore, a use for further purposes has to fulfil the legal requirements equal to a data transmission but there is an exemption for scientific or statistical purposes for which personal data may be used under certain conditions.

Personal data may be further used for scientific and statistical purposes under one of the following conditions:

- the data is publicly available;
- the data was initially collected legitimately by the controller for other purposes;
- the data is used only in a pseudonymous form;
- the data is used for these purposes pursuant to a legal provision;
- the data subject has given his consent;
- the Data Protection Authority has given its approval.

Nevertheless, also in case of a legitimate use of personal data for scientific or statistical purposes according to one of the conditions mentioned above, this data has to be transformed into a pseudonymous form immediately if pseudonymous data is sufficient to serve the research's purposes as well. As long as it is not stated

otherwise by law, data must be anonymised immediately if the personal identity of the data subjects concerned is no longer relevant.

Security obligations

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

The imposed security obligations are as follows:

- distribution of functions between the organisational units, as well as the operatives regarding the use of data, has been laid down expressly;
- use of data has been tied to valid orders of the authorised organisational units or operatives;
- every operative employee has been instructed about his or her duties of confidentiality pursuant to the ADPA and to internal data protection regulations including data security regulations;
- operation of an access control system for objects of the data controller or data processor;
- operation of an access control system for the protection of data and programs as well as for the protection of storage media against unauthorised access and use;
- the permissions to operate data processing equipment has been defined and every device has been secured against unauthorised operation by taking security measurements for the machines and programs used;
- creation of log files in order to monitor the legitimacy of the use of personal data like retrieval, modifications and transmissions; and
- establishment of an appropriate documentation about the measures taken pursuant to the previous bullet points to facilitate control and conservation of evidence.

Although all these security measures to be taken seem very comprehensive, they usually do not impose a large burden on data controllers as they are not examined by the DPA with high scrutiny.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

An amendment to the DPA in 2010 introduced a 'data breach notification' duty for controllers that have failed to keep their hosted data secure; if the controller becomes aware of any systematic and grave misuse of any data that might cause harm to the affected data subjects, it has the obligation to adequately inform the data subjects thereof. This obligation is usually fulfilled by written statements to the subjects, which provide them with the information of the security breach, the data affected, any recipient of the data (if known) and the possible dangers resulting from the breach. It is not required by law to inform the regulator of any breach.

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

There is generally no rule for appointing a mandatory data protection officer, so the appointment of a data protection officer is not mandatory. Rules for a non-mandatory data protection officer are still in political discussion.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Owners of PII are required to establish internal processes and documentation in order to ensure the rights of individuals regarding their data (see question 34). Equal measures have to be taken by all organisational units of a data controller or data processor that use data in order to ensure data security.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

Once a company processes personal data (relating to its employees, customers or any other natural or legal persons) the company must register as a data controller and notify its data applications with the DPA. There are only a few exceptions, the most important of which are the 'standard applications', which are regularly published as a regulation by the Federal Chancellor of Austria and determine in detail which categories of data may be processed and transmitted lawfully. If a data application can be completely subsumed under such a standard application, the duty to notify or register is lapsed.

The exemptions from the duty to inform data subjects as mentioned in question 13 also apply for the duty of registration with the DPA.

24 Formalities

What are the formalities for registration?

The data controller has to file a notification with the Data Processing Register, including information about the data controller's company, commercial register number, its address, postal address and telephone number. In addition, for each data application the data controller has to notify the purpose of the application, its legal basis, the categories of data subjects concerned, the data categories processed, all data security measurements implemented and, if any, recipients of personal data. All this data has to be kept up to date and any changes have to be filed with the Data Processing Register immediately. If special categories of data are to be processed (see question 11), the DPA's prior authorisation is necessary. No notification fees are charged.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

If an application is operated without being registered appropriately or without being registered at all, a fine of up to €10,000 may be imposed on the data controller.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The Data Processing Register may initiate an improvement process if data controller's notification is found insufficient, incorrect or even unlawful. If the data controller does not improve its notification within the determined period, the registration of the notification will be refused.

27 Public access

Is the register publicly available? How can it be accessed?

The Public Data Processing Register may be consulted by anyone online at https://dvr.dsk.gv.at/at.gv.bka.dvr.public/DVRRecherche.aspx. It is also possible to receive information via e-mail or telephone. The contact details are:

Datenverarbeitungsregister
Hohenstaufengasse 3
1010 Vienna
Austria
Tel: +43 1 531 15 / 204043
Fax: +43 1 531 15 / 204016
dvr@dsk.gv.at.

28 Effect of registration

Does an entry on the register have any specific legal effect?

Once a data controller has registered with the Data Processing Register, it is obliged to keep any data updated and to inform the Data Processing Register of any new information or amendments to data notifications (see also question 12 et seq). If special categories of data are to be processed (see question 11), the DPA's prior authorisation is necessary and is granted with the registration.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

Controllers may employ processors for their data applications insofar as the latter sufficiently warrant the legitimate and secure use of data. Therefore, the controller must enter into the necessary agreements with the processor in order to enforce the data processor to have all data security measurements being implemented required by law.

Irrespective of further contractual obligations, all processors have the following obligations when processing personal data on behalf of the controller:

- data may only be used according to the instructions of the controller;
- compulsory data safety measures have to be taken (see question 22);
- another processor may only be engaged with the prior permission of the controller and the controller has to be informed of any intended engagement of another processor;
- technical and organisational measurements have to be implemented for the fulfilment of the controller's obligation to grant the right of information, rectification and erasure;
- all results from the processing and all documentation data have to be returned to data controller after the termination of service; and
- all information necessary for the data controller to enable him or her to examine if the data processor has discharged its obligations arising from the engagement has to be provided to the data controller.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

According to the ADPA, data must only be used fairly and lawfully, only be collected for specific, explicit and legitimate purposes and be used insofar as they are essential for the purpose of the data application. In addition, data must only be processed insofar as the purpose and content of the data application are covered by the statutory competencies or the legitimate authority of the respective controller and the data subject's secrecy deserving protection is not infringed.

Non-sensitive personal data may be processed if one of the following conditions is met:

- an explicit legal authorisation or obligation exists to use the data;
- the data subject has unambiguously given his or her consent, which can be revoked at any time, whereby such a revocation makes any further use of the data illegal;
- vital interests of the data subject or prevailing interests pursued by the controller or by a third party require the use of data; and
- the use of legitimately published data and merely indirect (pseudonymous) personal data will not constitute an infringement of interests in secrecy deserving protection (the right to object to the use of such data remains unaffected).

If sensitive data is processed, secrecy is not infringed if:

- the data subject has clearly made the data public him or herself;
- the data is used only in an indirect (pseudonymous) personal form;
- the obligation or authorisation to use the data is stipulated by law, insofar as it serves an important public interest or they are used by a controller in the public sector in fulfilment of its obligation to give the authorities assistance;
- data is used that solely concerns the execution of a public office by the data subject;
- the processing or transmission is in the vital interest of the data subject and his or her consent cannot be obtained in time;
- the use is in the vital interest of a third party;
- the use is necessary for the establishment, exercise or defence of legal claims of the controller before a public authority and the data were collected legitimately;
- the data is used for private or research purposes or in case of disaster;
- the use is required according to the rights and duties of the controller in the field of employment law and civil service regulations and is legitimate pursuant to specific legal provisions (the rights of the labour councils according to the Labour Constitution Act with regard to the use of data remain unaffected);
- the data is required for the purpose of preventive health care, medical diagnosis, the provision of health care or health treatment or the management of health-care services, and the use of data is performed by a medical person or other persons subject to an equivalent duty of secrecy; or
- non-profit organisations with a political, philosophical, religious or trade union aim process data revealing the political opinion or philosophical beliefs of natural persons in the course of their legitimate activities, as long as these data concern members, sponsors or other persons who disclose an interest in the aim of the organisation on a regular basis; these data shall not be disclosed to a third party without the consent of the data subject unless otherwise provided for by law.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Data transfers from Austria to any other EEA member states are not subject to any additional requirements, as EEA member states are considered to provide an 'adequate level of data protection'.

Also, data transfers to recipients in third countries providing an adequate level of data protection do not need to fulfil any further requirements. All jurisdictions that are not a member of the EEA but provide an adequate level of data protection are enumerated in a regulation of the Federal Chancellor (Federal Law Gazette II No 521/1999 as amended by No 150/2013) and are listed here: Andorra; Argentina; Faroe Islands; Guernsey; Isle of Man; Jersey; New Zealand; Switzerland; and Uruguay.

Pursuant to this regulation, a data transfer to one of the following countries does not require the Data Protection Authority's prior approval, but only under specific conditions as stated in the regulation: USA (if the data recipient is Safe Harbor-certified); Canada; and Israel.

Furthermore, any applicable decision of the European Commission is binding in Austria.

In any case, a trans-border data exchange does not require the DPA's prior authorisation if:

- the data to be transferred has been published legitimately in Austria;
- only indirect personal (pseudonymous) data is transferred;
- the trans-border transfer is authorised by legal provisions that are equivalent to a provision of the Austrian legal system and are immediately applicable;
- data out of a data application for private or journalistic purposes are transmitted;
- the data subject unambiguously has given his or her consent to the trans-border data transmission;
- a contract has been concluded between the controller and the data subject or the controller and a third party clearly in the interests of the data subject which cannot be fulfilled without the trans-border transmission of data;
- the transmission is necessary for the establishment, exercise or defence of legal claims before a foreign authority and the data was collected legitimately;
- the transmission is expressly mentioned in a standard application or model application;
- the data exchange is carried out with Austrian governmental ministries and offices in foreign countries; or
- the transmission concerns personal data out of a data application that is exempted from the notification duty pursuant to section 17 paragraph 3 ADPA.

If the trans-border data exchange is not exempted from a prior authorisation duty, the controller has to apply for authorisation to the DPA. In the context of trans-border data flows to countries which do not provide an adequate level of data safety, data transfer agreements are very important. To receive the DPA's approval for the transfer of personal data to these countries, it is necessary that the controller provides for sufficient guarantees to ensure an adequate level of data protection. Such an adequate level of data protection could be established by the conclusion of data transfer agreements based on the European Commission's standard contractual clauses. A precise distinction needs to be made between Controller-to-Controller and Controller-to-Processor clauses. If such agreements are concluded using the standard contractual clauses as published by the European Commission, the probability of receiving the DPA's authorisation is quite high.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

If a data application is not exempted from the duty of notification at all, data transfers have to be filed with the DPA as well. Such a notification has to be carried out together with the filing of the data application itself via DVR-Online.

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Restrictions to transfers outside the jurisdiction do apply, if the data recipient is located outside the EEA. If a data transfer is not exempt from the authorisation duty according to question 31, the controller has to apply for prior approval from the Data Protection Authority. The DPA may grant its authorisation under specific conditions and obligations.

The same restrictions apply to data transfers to service providers.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

Data subjects have the right to access their personal data processed by controllers and to receive a copy. The data controller is obliged to provide the data subject with information about personal data being processed, if the data subject has to request access in writing and how the data subject must prove his or her identity, as appropriate (eg, by transmitting a passport copy). If there is no reason to refuse a data subject's request, the desired information has to be disclosed within eight weeks upon receipt.

Information shall not be disclosed to the data subject if this is necessary for the protection of the data subject because of special reasons or if legitimate interests pursued by the data controller or by a third party – especially overriding public interests – prevail furnishing the information. Prevailing public interests are the following:

- protection of the constitutional institutions of Austria;
- safeguarding the operational readiness of the Federal Army;
- safeguarding the interests of a comprehensive national defence;
- protection of important foreign-policy, economic or financial interests of the Republic of Austria or the European Union; or
- prevention and prosecution of crimes.

The review of the legitimacy of a refusal of the provision of the requested information because of one of these reasons is subject to a decision of the DPA.

35 Other rights

Do individuals have other substantive rights?

Besides the right of access, individuals have the right to apply for rectification and deletion of personal data relating to them if this data is inaccurate. Finally, individuals have the right to raise objections to the data controller of the data application against the use of personal data because of infringement of the data subject's overriding interest in secrecy deserving protection arising out of any special situation.

Every data subject has the right to lodge a complaint with the DPA because of an alleged infringement of his or her rights.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals are entitled to demand compensation if they are affected by breaches of data protection law. A person who has been damaged by an infringement of provisions of the ADPA (confidentiality, correction, erasing) may take a civil action for damages. In general, compensation may only be demanded for actual damages, but there is an exception pursuant to section 33 ADPA, which states that a claim for appropriate compensation for the defamation suffered may be brought against a data controller if the personal data was used publicly in a manner that violated a data subject's interests in secrecy exposing that person to the extent similar to that described in section 7 paragraph 1 of the Media Act, Federal Law Gazette No. 314/1981 – even if public use of that data is not committed by publication in the media.

Update and trends

In 2012 Austria was convicted by the European Court of Justice for the lack of independence of the Austrian Data Protection Commission. As a consequence, the Austrian Data Protection Act (ADPA) was amended by the ADPA Amendment 2013 to ensure and guarantee the independence of this authority by law. Since then, the authority is now an independent government department by law and must be provided with adequate staffing and resources. The Federal Chancellor still has the right to be informed about the authority's affairs, but this right of information was reduced to the extent that it does not conflict with the authority's independence.

In May 2013, a second amendment of the ADPA came into force which transforms the current Data Protection Commission into the Data Protection Authority (ADPA Amendment 2014). This amendment integrates the Data Protection Authority into the new system of administrative courts to be established on 1 January 2014. From this date, appeals to the newly installed Federal Administrative Court are possible and the trinomial stages of appeal will come into being. The responsibility for decisions at the Federal Administrative Court in data protection matters will pass to a senate consisting of a judge and two lay judges, each a representative of the Austrian Federal Economic Chamber and the Austrian Federal Employee Chamber. Proceedings pending with the Data Protection Commission at the end of 2013 will be seamlessly continued by the newly established Data Protection Authority.

In case indications arise that a serious data protection infringement has been committed by a private sector controller, besides the data subject, the DPA is also empowered to file an action for a declaratory judgment with the responsible court.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

The rights of individuals are enforceable through either the DPA or the judicial system, but the responsibility depends on if the data controller is established by public or private law. Complaints against data controllers of the public sector have to be filed with the DPA, while claims against data controllers of the private sector have to be filed with the responsible court.

Pursuant to section 30 ADPA, anyone has the right to lodge an application with the DPA because of an alleged infringement of his or her rights pursuant to the ADPA by a controller or a processor.

Pursuant to section 31 ADPA, actions for infringement of the right to secrecy, rectification and erasure against data controllers established in forms of public law are to be brought before the DPA as long as the complaint shall not be brought against organs of the legislative or jurisdiction. This also applies for any data controller for actions of infringement of the right to access personal data independent from its form of establishment. Pursuant to section 32 ADPA, actions for infringement of the right to secrecy, rectification and erasure against natural persons, groups of persons or legal entities established in forms of private law are to be brought before the civil courts.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

No.

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

Data controllers currently may appeal to the Supreme Administrative Court. After 1 January 2014, data subjects may appeal against decisions of the DPA to the Federal Administrative Court which will be established on this date, and may further appeal against decisions of the Federal Administrative Court to the Supreme Administrative Court.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

To protect data and computer systems the Criminal Code contains rules that stipulate high fines and even imprisonment. In addition, the ADPA contains one provision that may lead to imprisonment for up to one year if somebody, with the intention to profit or to harm others, uses, publishes or makes available to others personal data which was entrusted or made accessible to him or her solely for professional reasons or which he or she acquired illegally him or herself.

PRESLMAYR
RECHTSANWÄLTE

Rainer Knyrim **knyrim@preslmayr.at**

Universitätsring 12
1010 Vienna
Austria

Tel: +43 1 533 16 95
Fax: +43 1 535 56 86
www.preslmayr.at

41 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

These issues have to be evaluated under general principles and according to the provisions of the ADPA respectively the Telecommunications Act. As the EU e-Privacy Directive 2002/58/EC has been amended by Directive 2009/136/EG, new special regulations for the declaration of consent for the use of cookies on websites had to be translated to the Telecommunications Act.

Austria implemented the EU e-Privacy Directive in November 2011 and has simply translated article 5 paragraph 3 of the Directive into section 96 paragraph 3 Telecommunications Act.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Both the Telecommunications Act and the e-Commerce Act contain provisions for commercial communications and sanctions for 'cold calling' and unsolicited faxes and e-mails. Commercial calls and the transmission of commercial messages are only legitimate with the recipient's prior consent. Some exceptions exist for the transmission of e-mails. Violating these provisions could lead to a fine with a fee of up to €37,000.