ICLG

The International Comparative Legal Guide to:

Data Protection 2014

1st Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

BANNING
Barrera, Siqueiros y Torres Landa, S.C.
CMS Reich-Rohrwig Hainz
Dittmar & Indrenius
DLA Piper
ECIJA ABOGADOS
Eversheds
Gilbert + Tobin Lawyers
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
KALO & ASSOCIATES
Koep & Partners
Marrugo Rivera & Asociados, Estudio Jurídico
Matheson
Mori Hamada & Matsumoto
Opice Blum, Bruno, Abrusio e Vainzof Advogados Associados
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Portolano Cavallo Studio Legale
Raja, Darryl & Loh
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Account Managers
Edmond Atta, Beth Bassett, Antony Dine, Susan Glinska, Dror Levy, Maria Lopez, Florjan Osmani, Paul Regan, Gordon Sambrooks, Oliver Smith, Rory Smith

Sales Support Manager
Toni Wyatt

Sub Editors
Nicholas Catlin
Amy Hirst

Editors
Beatriz Arroyo
Gemma Bridge

Senior Editor
Suzie Kidd

Global Head of Sales
Simon Lemos

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
May 2014

ISBN 978-1-908070-98-2
ISSN 2054-3786

Strategic Partners

General Chapter:

Country Question and Answer Chapters:

Further copies of this book and others in the series can be ordered from the publisher. Please call +44 20 7367 0720

EDITORIAL

Welcome to the first edition of *The International Comparative Legal Guide to: Data Protection*.

This guide provides the international practitioner and in-house counsel with a comprehensive worldwide legal analysis of the laws and regulations of data protection.

It is divided into two main sections:

One general chapter entitled *Data Protection – a Key Business Risk*.

Country question and answer chapters. These provide a broad overview of common issues in data protection laws and regulations in 29 jurisdictions.

All chapters are written by leading data protection lawyers and industry specialists and we are extremely grateful for their excellent contributions.

Special thanks are reserved for the contributing editor Bridget Treacy of Hunton & Williams for her invaluable assistance.

Global Legal Group hopes that you find this guide practical and interesting.

The *International Comparative Legal Guide* series is also available online at www.iclg.co.uk.

Alan Falach LL.M.
Group Consulting Editor
Global Legal Group
Alan.Falach@glgroup.co.uk

Austria

Dr. Sonja Hebenstreit

Herbst Kinsky Rechtsanwälte GmbH

Dr. Isabel Funk-Leisch

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation in Austria is the Federal Act concerning the Protection of Personal Data (*Bundesgesetz über den Schutz personenbezogener Daten Datenschutzgesetz 2000* – hereinafter referred to as "DSG 2000"). It applies to both the private and public sector.

1.2 Is there any other general legislation that impacts data protection?

Data Protection is impacted by labour law. The principal legislation on data protection regarding labour law is the Works Council Constitution Act (*Arbeitsverfassungsgesetz* – hereinafter referred to as "ArbVG"), in particular sections 96 and 96a ArbVG. For certain Data Applications the consent of the works council is mandatory.

1.3 Is there any sector specific legislation that impacts data protection?

Other sector specific legislation can e.g. be found in the Telecommunications Act 2003 which contains the implementation of the EU Data Protection Directive on Electronic Communications (e.g. provisions regarding commercial electronic communication, cookies, etc.), as well as in the Banking Act (banking secrecy).

1.4 What is the relevant data protection regulatory authority(ies)?

The relevant Austrian data protection authority is the "*Datenschutzbehörde*" (in the following referred to as DSB); the DSB is also responsible for the Data Processing Register (*Datenverarbeitungsregister*) which has been established within the DSB. For details concerning the competences of the DSB see sections 4 and 5. Another institution is the Data Protection Council (*Datenschutzrat*) which is responsible to advise the Federal Government and the State Governments on requests concerning data protection law (section 41 para 2 DSG 2000).

2 Key Definitions under Austrian Law

2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  Personal Data is defined as information relating to Data Subjects who are identified or identifiable.

- **"Sensitive Personal Data"**

  Sensitive Data concerns a particular category of data deserving special protection. Sensitive Data comprises data relating to natural persons concerning their racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership and their health or sex-life.

  The use of Sensitive Data is severely restricted and only permitted for reasons stipulated in section 9 DSG 2000.

- **"Processing"**

  Processing of data means the collection, recording, storing, reproduction or any other kind of operation with data except for the transmission.

- **"Data Controller"**

  Data Controller is a natural or legal person, a group of persons or organ of a federal, state or local authority (*Gebietskörperschaft*) or the offices of these organs. The Data Controller is entitled to decide (alone or jointly with others) on the use of data, irrespective of whether the Data Controller uses the data himself or authorises a Data Processor thereto.

- **"Data Processor"**

  Data Processor is a natural or legal person, a group of persons or organ of a federal, state or local authority (*Gebietskörperschaft*) or the offices of these organs, if they use data only for a commissioned work on behalf of the Data Controller.

- **"Data Owner"**

  The DSG 2000 does not use the definition "Data Owner". The rights of a Data Owner yield the rights of the Data Controller according to DSG 2000.

- **"Data Subject"**

  Data Subject (*Betroffener*) is any natural or legal person or group of natural persons not identical to the Data Controller, whose data are processed.

- **"Pseudonymous Data"**

  DSG 2000 does not use the definition "Pseudonymous Data". However, DSG 2000 defines "Indirect Personal Data", which is given in case the identity of the Data Subject is not known to the particular Data Controller using such data, but the data is not anonymous data. Therefore, data are only "indirectly personal" when the identity of the Data Subject cannot be determined by the Data Controller, Data Processor or recipient of a Transmission with legally admissible means.

- **"Direct Personal Data"**

  Please refer to Personal Data above.

- **"Consent"** is defined as the valid declaration of intention of a Data Subject, given without constraint, that he/she agrees to the use of data relating to him/her in a given case, after having been informed about all relevant facts.

- **"Joint Information System"** (*Informationsverbundsystem*) describes joint processing of data in a Data Application by several Data Controllers and the joint utilisation of the data so that every Data Controller has access even to those data in the system that have been made available to the system by other Data Controllers.

- **"Transmission"**

  Transmission of data means the transfer of data to recipients other than the Data Subject, the Data Controller or a Data Processor, in particular this term refers to the publishing of data, but also to the use of data for another application purpose of the Data Controller.

- **"Committing"**

  Committing of data is the transfer of data from the Data Controller to the Data Processor in the context of a commissioned work.

- **"Data Application"**

  A Data Application is the sum of logically linked stages of use of data which are organised in order to reach a defined result and which are as a whole or partially performed automatically.

3 Key Principles

3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  According to section 6 DSG 2000, data shall only be used fairly and lawfully and only be collected for specific, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. The Data Controller shall bear the responsibility that these principles are complied with in all his Data Applications; even when employing a Data Processor to use the data.

- **Lawful basis for processing**

  According to section 7 para 1 DSG 2000 data shall 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 Data Controller and the Data Subjects' interest in secrecy deserving protection is not infringed.

  Pursuant to section 8 DSG 2000 interests in secrecy deserving protection are not infringed when using non-sensitive data if an explicit legal authorisation or obligation to use the data exists or the Data Subject has given his consent (which can be revoked at any time) or vital interests of the Data Subject require their use or overriding legitimate interests pursued by the Data Controller or by a third party also require the use of data.

- **Purpose limitation**

  According to section 7 para 3 DSG 2000 the legitimacy of a use of data requires that the intervention be carried out only to the extent required, and using the least intrusive of all effective methods and that the principles of section 6 DSG 2000 be respected.

- **Data minimisation**

  Please see above under "Purpose limitation".

- **Proportionality**

  Please see above under "Purpose limitation".

- **Retention**

  According to section 6 para 1 DSG 2000 data shall only be kept in a form which permits identification of Data Subjects as long as this is necessary for the purpose for which the data were collected.

- **Correctness and completeness**

  According to section 6 para 1 sub-para 4 DSG 2000 data may only be used so that the results are factually correct with regard to the purpose of the application, and the data must be kept up to date when necessary.

4 Individual Rights

4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data – right to information**

  According to section 26 para 1 DSG 2000 a Data Controller shall provide any person or group of persons with information about the data being processed about the person or the group of persons who so request in writing and prove his/her identity in an appropriate manner. Subject to the agreement of the Data Controller, the request for information can be made orally. The information shall contain the data processed, the information about their origin, the recipients or categories of recipients of Transmissions, the purpose of the use of data as well as its legal basis in intelligible form.

  Upon request of a Data Subject, the names and addresses of processors shall be disclosed in case they are charged with Processing Data relating to him. If no data of the person requesting information exists, it is sufficient to disclose this fact (negative information).

  With the consent of the person requesting information, the information may be provided orally alongside the possibility to inspect and make duplicates or photocopies instead of being provided in writing.

  The information shall not be given insofar as this is essential for the protection of the person requesting information for special reasons or insofar as overriding legitimate interests pursued by the Data Controller or by a third party, especially overriding public interests, are an obstacle to furnishing the information pursuant to section 26 para 2 DSG 2000.

- **Correction and deletion**

  According to section 27 para 1 DSG 2000 every Data Controller shall rectify or erase data that are incorrect or have been processed contrary to his own, as soon as the incorrectness of the data or the inadmissibility of the processing becomes known to him, or due to a well-founded application by the Data Subject.

  The application for rectification or erasure shall be complied with within eight weeks after receipt and the applicant shall be informed thereof, or a reason in writing shall be given stating why the requested erasure or rectification was not carried out pursuant to section 27 para 4 DSG 2000.

- **Objection to processing**

  According to section 28 DSG 2000 every Data Subject shall have the right to raise an objection with the controller of the Data Application against the use of data because of an infringement insofar as the use of data is not authorised by law.

  If the requirements are met, the Data Controller shall erase the data relating to the Data Subject within eight weeks from his Data Application and shall refrain from transmitting the data.

- **Objection to marketing**

  Objection to marketing activities is possible according to section 107 TKG – for further details please see section 7.

- **Complaint to relevant data protection authority(ies)**

  According to section 31 DSG 2000 the DSB shall decide on complaints of persons or a group of persons who allege to have been infringed in their right for information or in their right to be informed about an automatically processed individual decision insofar as the request for information (the application for information or disclosure) does not concern the use of data for acts in the service of legislation or jurisdiction.

- **Use of only indirectly personal data**

  According to section 29 DSG 2000 rights granted in sections 26 to 28 DSG 2000 cannot be exercised insofar as only indirectly personal data are used.

- **Information in case of serious misuse of data**

  According to section 24 para 2a DSG 2000, the Data Controller is, in case data from his Data Application are systematically and seriously misused and the Data Subject may suffer damages thereby, obliged to immediately inform the Data Subject in an appropriate manner (also see question 13.3 below).

  Such obligation does not exist if the information – taking into consideration that only minor damage to the Data Subject is likely and the cost of the information to all persons concerned – would require an inappropriate effort.

5 Registration Formalities and Prior Approval

5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

All Data Applications are subject to notification, unless an exception applies. Data Applications are not subject to notification if the Data Application contains solely published data (such as information made public by a company); or concerns the management of registers and catalogues that are by law open to access by the public; or contains only indirectly personal data; or is carried out by natural persons for entirely personal reasons or concerns just the person's family life; or is carried out for journalistic purposes according to section 17 para 2 DSG 2000.

Furthermore, certain applications concerning state security are not subject to notification according to section 17 para 3 DSG 2000. All the exceptions are regulated in section 17 para 2 and 3 DSG 2000.

If a large number of Data Controllers carry out the same Data Applications in a similar fashion which, due to the purpose of the use and the processed categories of data, is unlikely to be a risk to the data subjects' interest in secrecy, these Data Applications can be declared as standard applications (*Standardanwendungen*), which are not subject to notification either. Currently, 35 standard applications have been defined for different purposes of private and public data controllers, all of them exactly listing the data subjects and data which may be processed, as well as the potential recipients.

The current Standard Applications can be found in the *Standard- und Muster-Verordnung 2004 (StMV 2004)*, Federal Law Gazette II No. 312/2004.

5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Every Data Controller must notify all Data Applications used, unless an exception to the notification duty applies. Separate notifications need to be made for each data application detailing the relevant data subjects, the data categories used (e.g. name, address, social security number) as well as the purpose of use and the legal basis of the use of data. Furthermore, all recipients to whom data is transmitted and who are therefore regarded as Data Controllers according to DSG 2000 have to be detailed in the notification as well.

5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

Every Data Controller is obliged to notify a Data Application prior to processing with the DSB. The local Data Controller has to notify the use of a Data Application with the DSB in order to receive registration with the Data Processing Register. If a foreign legal entity has a branch office in Austria, the foreign legal entity has to register all Data Applications used in Austria.

The notification must be made in German and needs to be carried out electronically by using the web application provided by the DSB. Lawyers may directly use the web application; individuals may receive access by using a citizen card (*Bürgerkarte*). All registrations are publicly accessible.

5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)

A Data Application encompasses all categories of data (e.g. name, address, salary) processed about certain categories of Data Subjects (e.g. employees, customers). The notification has to state the categories of recipients – including possible recipients in countries outside the EEA – as well as the legal basis for the Transmission. The Data Controller has to provide the following information with the registration of a Data Application according to section 19 DSG 2000:

- the name (or other designation) and address of the Data Controller and of his representative according to section 6 para 3 DSG 2000;
- the registration number of the Data Controller;
- the proof of statutory competence or of the legitimate authority that the Data Controller's activities are permitted;
- the purpose of the Data Application and its legal basis;
- a general description of data security measures taken pursuant to section 14 DSG 2000;
- the categories of Data Subjects affected by intended transmissions, the categories of data to be transmitted and the

matching categories of recipients including possible recipients in third countries – as well as the legal basis for the transmission; and

- a statement explaining whether the Data Application requires prior approval by the DSB or not.

Furthermore according to section 8 of the Regulation on the Data Processing Register (*Datenverarbeitungsregister-Verordnung* 2012 – hereinafter referred to as "DVRV 2012") the Data Controller has to notify the DSB of the purpose of a Data Application about:

- his identity and the legal basis when first registering a Data Application;
- each notifiable Data Application;
- any changes of an already registered, notifiable Data Application (including the legal basis);
- any changes of the name or address of the Data Controller;
- if a reason for the deletion of a Data Application occurs; and
- if the appropriate legal basis for the registration of a Data Application no longer exists.

According to section 9 DVRV 2012 the information for a new or a change of registration regarding a Data Application are to be filled out completely in the Online-document of the respective "appendix 2"- formular (notification of a Data Application).

5.5 What are the sanctions for failure to register/notify where required?

The notification duties are laid down in section 17 DSG 2000. A failure to register/notify is deemed as an administrative offence and punishable by a fine of up to 10,000 Euros according to section 52 para 2 DSG 2000.

5.6 What is the fee per registration (if applicable)?

Notifications and registrations of data applications do not incur costs. Under section 53 DSG 2000, all applications for notification and for statements of the notified entry on the register are exempt from fees. The notification is carried out electronically by using the web application provided by the Data Protection Authority.

5.7 How frequently must registrations/notifications be renewed (if applicable)?

The Data Controller is obliged to keep his notifications always up to date. Changes and modifications for Data Applications which are already registered are to be notified to the DSB according to section 19 DSG 2000, as well as section 9 DVRV.

5.8 For what types of processing activities is prior approval required from the data protection regulator?

According to section 18 para 2 DSG 2000 prior approval by the DSB is required if the respective data application involves one or more of the following:

- sensitive data;
- data about the data subject's creditworthiness;
- data carried out in the form of a joint information system; or
- data about (judicial or administrative) offences according to section 8 para 4 DSG 2000.

According to section 12 DSG 2000 the Transmission and Committing of data to Member States of the EU/EEA as well as to countries with an adequate level of data protection (Switzerland, Canada, Argentina, Jersey, Guernsey, Isle of Man, Faroe Islands, Israel, Andorra, Oriental Republic of Uruguay and New Zealand) does not require authorisation.

In case of the Transmission and Committing of data to the United States of America the so called "Safe Harbour Agreement" applies to those companies, which voluntarily submit under the Safe Harbour Agreement. Transmitting and Committing of data to these companies must not be approved by the DSB.

Furthermore, certain exceptions to the approval apply according to section 12 para 3 if data shall be transmitted or committed outside the EU (e.g. data have been published legitimately in Austria or these data are only indirectly personal to the recipient).

In all other cases the transmission and committing is subject to approval by the DSB. For details please see question 5.9.

According to section 52 DSG 2000 fines may be expected in the case of Transmission without prior approval.

5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.

If prior approval is required for the data application, the procedure for prior approval starts automatically upon notification of a data application involving (e.g.) sensitive data, i.e. no separate application is required in that case.

Insofar as a case of transborder data exchange is not exempted from authorisation according to section 12 DSG 2000, the controller has to (separately) apply for approval from the DSB prior to the transmission or committing according to section 13 para 1 DSG 2000. The DSB can issue the approval subject to conditions and obligations.

The approval shall be given despite the lack of an adequate general level of data protection in the recipient state if:

- an adequate level of data protection exists for the transmission or committing outlined in the application for the permit in this specific case; and
- the Data Controller can satisfactorily demonstrate that the interests in secrecy deserving protection of the Data Subject of the planned data exchange will be respected outside of Austria. For this case, the concluding Standard Contractual Clauses (hereinafter referred to as "SCC") are applicable. The SCC have been published by the European Commission (Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council (notified under document C(2010) 593 – SCC for service providers)) and stipulate security measures and other duties to be fulfilled by the data receiving company seated in the country without an adequate level of data protection.

In the case of Data Applications subject to notification, the DSB shall put a copy of each ruling authorising the transborder transmission or committing of data on the notification file and enter the fact that authorisation has been granted into the Data Processing Register.

The procedure for obtaining prior approval may last from 2 to 36 months.

6 Appointment of a Data Protection Officer

6.1 Is the appointment of a Data Protection Officer mandatory or optional?

The appointment of a Data Protection Officer is not a legal

requirement under Austrian law. However, every data controller is free to appoint such Data Protection Officer.

6.2 What are the sanctions for failing to appoint a mandatory Data Protection Officer where required?

This is not applicable.

6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?

A Data Protection Officer shall guarantee the compliance with the use of Personal Data and the fulfilment of legal requirements. The appointment of a Data Protection Officer provides no direct advantages under Austrian law.

6.4 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable.

6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?

As set out above, Austrian law does not require the appointment of a Data Protection Officer.

Typically, the main responsibilities of the (optional) Data Protection Officer comprise of the following:

- Supervision and control of compliance with the legal and internal requirements regarding the use of personal data.
- DSB notification requirements.
- Consultancy and training in relation to data protection and data security.

In order to fulfil his duties properly the Data Protection Officer shall:

- be free from instructions and external influence in the application of the DSG 2000 and have the right to inspect all relevant and necessary documents;
- be provided with appropriate equipment and means;
- have the right to call in specialists to answer specific questions;
- have a direct right of control in all areas of the company; and
- have a right of initiative and opposition in case of reasonable suspicion of an or committed infringement of the DSG 2000.

6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

No registration or notification of the Data Protection Officer with the DSB is required. The appointment of a Data Protection Officer only requires the consent of the respective employee. A written appointment is recommended.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, or SMS text message. (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)

According to section 107 para 1 TKG, calls, including facsimile transmissions, for marketing purposes shall not be permitted without the prior consent of the subscriber. Please note that prior consent may not be received in the course of the first call, but needs to be given before.

According to section 107 para 2 TKG the sending of electronic mail – including SMS messages – without the recipient's prior consent shall not be permitted if the sending takes place for purposes of direct marketing or is addressed to more than 50 recipients. Such prior consent shall not be required, if:

- contact details for the communication were obtained in the context of a sale or a service to the recipient;
- the communication is transmitted for the purpose of direct marketing of his own similar products or services; and
- the recipient clearly and distinctly has been given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details and the recipient did not register in the "Robinson List" (section 7 ECG).

For reasons of clarity, it is advisable to get prior consent of the recipient for any marketing activities through email or SMS.

7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The competent authority for the enforcement of section 107 TKG is the Telecommunications Authority ("*Fernmeldebehörde*"). The authority mainly becomes active upon complaints by persons.

Further, the misuse of an email address not publicly known may constitute a violation of data protection law which may be sanctioned with administrative fines according to the DSG 2000, rendered by the respective regional administrative authority ("*Bezirksverwaltungsbehörde*").

7.3 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The infringement of section 107 para 2 (emails/SMS for marketing purposes without consent) TKG constitutes an administrative offence which is punishable by a fine of up to 37,000 Euros.

The infringement of section 107 para 1 (calls/fax for marketing purposes without consent) TKG constitutes an administrative offence which is punishable by a fine of up to 58,000 Euros.

7.4 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

Cookies containing personal data require the consent of the subscriber. The subscriber has to be informed on which legal basis and for which purposes this will take place and for how long the data will remain stored (section 93 para 3 TKG). The consent required according to section 96 para 3 TKG is different from the explicit consent according to DSG. Consent given by the subscriber within the browsing adjustments after commencing the use of the website is considered adequate for the purpose of section 96 para 3 TKG, the necessary information can be provided within the legal details of the website. Behavioural Advertising is always subject to consent according to section 96 para 3 TKG.

However the Article 29 Data Protection Working Party (WP) recently published a Working Document 02/2013 providing guidance on obtaining consent for cookies. According to WP the use of cookies is subject to the prior information and the consent of the user. Consent has to be provided freely, unambiguously and by

the user's active action. Following WP, the consent to the use of cookies containing personal data has to be an explicit opt-in consent. The opinion of WP is not mandatory but it is usually used by the relevant authorities to determine the content of data protection legislation, in this case of section 96 para 3 TKG and the consent necessary thereby.

7.5 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

Please see question 7.4.

7.6 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

We are not aware of any publicly known enforcement action in this respect.

7.7 What are the maximum penalties for breaches of applicable cookie restrictions?

An infringement of section 96 para 3 TKG constitutes an administrative offence which is punishable by a fine of up to 37,000 Euros.

8 Restrictions on International Data Transfers

8.1 Please describe any restrictions on the transfer of personal data abroad.

The first prerequisite for the assessment of permissibility of each transfer (transmission or committing) of data to a third person is the lawful use of data in the context of the respective data application and (if no exception applies) the notification of the data application.

Further it needs to be examined whether the transfer of data to a recipient outside Austria requires prior approval of the DSB. No such approval is required for the transfer of data to a recipient within the European Economic Area. Furthermore, transfer of data to a recipient outside of the European Economic Area requires no permission, if the third country provides for an adequate level of data protection. Currently, transfer to Switzerland, Canada, Argentina, Uruguay, Israel, Isle of Man, Faroe Islands, Andorra, Guernsey and New Zealand as well as to Safe Harbour certified recipients in the USA does not require prior approval of the DSB.

If the transfer is made to recipients in other countries, prior approval of the DSB for such transfer is in principle necessary unless an exemption applies (e.g. the data subject has expressly agreed to the transfer of its data to the respective recipient abroad, a contract concluded between data subject and controller primarily in the interest of the data subject may only be fulfilled by transfer of the data abroad, the transfer is mentioned in a standard regulation, etc.).

If no exemption applies and the transfer is made within a group of companies under Binding Corporate Rules or the recipient has accepted the EU Standard Model Clauses, the data controller still needs to apply for approval but such approval will in general be granted (also in principle within a shorter period of time; also see questions 5.8 and 5.9 above).

8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Given the above restrictions, it is advisable to use data processors (service providers) in a country with an adequate level of data protection or a safe harbour certificate, if applicable, and/or to install Binding Corporate Rules if data generally needs to be sent to recipients outside the EEA and to third countries without an adequate level of data protection within a group of companies.

8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.

An application for approval of a transfer of data abroad according to section 13 DSG 2000 has to be applied for with the DSB. The DSB might require that the respective Data Processing Agreement (if applicable) containing the Standard Model Clauses and or further documentation necessary for the assessment of the legality of the transfer is provided to the authority. The timeframe for the decision may vary between 2 to 36 months (also see questions 5.8 and 5.9 above).

9 Whistle-blower Hotlines

9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)

Austrian law does not contain specific provisions referring to whistle-blower systems, but the DSB has rendered several decisions on the installation of whistleblowing systems. As the subject of a report of employees through whistleblowing systems – misconduct of or violation of the law or internal guidelines by an employee – will (in most cases) be data concerning acts and omissions punishable by the courts or administrative authorities, and in particular concerning suspected criminal offences, the use of such data requires the prior examination and approval of the DSB. In the following, we refer to the reported behaviour as "misconduct".

The DSB has rendered several decisions on the installation of whistleblowing systems. The DSB has in the past approved the use of data in the context of a whistleblowing system only under the following conditions:

- notifications of misconduct on an anonymous basis are admitted, but not encouraged by the data controller;
- the department dealing with the notifications must strictly be separated from any other department and the staff of such department must be skilled and explicitly in charge of treating the personal data as confidential;
- persons being under the suspicion of having committed any severe misconduct must be granted access to all information supporting or evidencing the allegations;
- the identity of the whistle-blower may only be disclosed if his/her allegations were knowingly wrong; and

- any personal data obtained by means of the whistleblowing system must be deleted within two months after the completion of the respective inquiry.

The transfer of data collected through the whistleblowing system to a foreign holding company located in a country outside the EEA if such country only provides for an inadequate level of protection under EU law has been approved by the DSB only for the following data and under the following additional conditions:

- data concerning executive employees and similar responsible employees (*leitende Angestellte und vergleichbar verantwortliche Personen*) who are accused of a misconduct;
- data concerning employees of the data controller who used the system for the report of a misconduct and identified themselves;
- data concerning employees of the data controller and other holding companies who were named as witnesses, informants or otherwise involved persons in the course of the use of the system;
- data concerning local employees who are not executives may not be transferred to the foreign holding company. This data may only be used on a local level; and
- the data controller has concluded a contract with the service provider of the system in order to ensure that only contents approved by DSB are transferred to the foreign holding company.

Moreover, in general, an agreement with the works council is required for the implementation of a whistleblowing system. The DSB has in the past required that such works council agreement should be provided to the authority or has granted approval only under the condition that a works council agreement is concluded.

9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?

As detailed above, the DSB states that notifications of misconduct on an anonymous basis are admitted, but should not be encouraged by the data controller.

9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.

Yes. As set out in question 9.1, prior approval of the DSB is required before the whistle-blower hotline may be implemented. Furthermore – if data is transferred to a country not providing for an adequate level of data protection – a separate approval by the DSB for transfer outside the EEA might be necessary. For the requirements as to the content of whistle-blower hotlines, see question 9.1 above. Please note that the timeframe for DSB's approval has in the past been several years.

10 CCTV and Employee Monitoring

10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?

Yes. In case a CCTV processes picture data, such processing is regarded as a data application processing personal data (as the persons on the videos might be identified through their picture) which in principle requires notification with the DSB prior to starting the processing unless the data controller ensures that the video surveillance data is encrypted and will only be analysed by a specific institution in specific cases and the sole code key is provided to the DSB (then a simple notification suffices).

Further, the law explicitly requires that in case works council agreements are required according to section 96a of the Labour Constitution Act 1974 - ArbVG, Federal Law Gazette No. 22, these need to be submitted to the DSB in the registration procedure.

Video surveillance is exempted from the notification obligation:

- in cases of real-time observation; or
- if the recording is only made on an analog video recording system.

The controller of a video surveillance is obliged to put up appropriate signs in order to inform the data subjects about the video surveillance.

The DSB has in its sections 50a *et seq.* laid down the principles under which video surveillance is permitted.

"Video surveillance" under Austrian law means the systematic and continuous observation of occurrences concerning a certain object (observed object) or a certain person (observed person) by technical devices designed to make or transmit images.

Lawful purposes for video surveillance, especially analysis and transmission of the data obtained in such way, only are the protection of the object or the person observed or the fulfilment of legal duties of diligence, including securing of evidence.

Video surveillance does not infringe the interests for secrecy deserving protection of the data subject mainly if:

- it is made in the vital interest of a person; or
- the data subject has expressly consented to the use of its data in the context of the surveillance operation.

In case the video-surveillance is not made in the performance of official executive tasks (i.e. for private purposes), it does not infringe the interests for secrecy deserving protection of the data subject if:

- certain facts justify the presumption that the object or person observed could become the target or the location of a dangerous attack;
- directly applicable legal rules of international or EU law oblige the controller to special duties of diligence for protection of the object or the person observed; or
- the surveillance is restricted to a mere real time reproduction of occurrences concerning the observed object/the observed person which, therefore, are neither recorded nor processed in any other way (real time surveillance) and is performed for the purpose of the protection of health, life or property of the controller.

Furthermore, the law justifies transfer of data recorded by video surveillance:

- to the competent authority or the court, if the controller has reasonable ground for suspicion that the data could document a criminal act punishable by the courts to be prosecuted *ex officio*; or
- to police authorities in order to carry out their function granted under the Police Act (SPG) Federal Law Gazette No. 566/1991, even if the action or attack is not directed against the object or the person observed.

Any use of video surveillance must be documented. This does not apply to real time observation.

10.2 What types of employee monitoring are permitted (if any), and in what circumstances?

Section 50a para 5 DSG 2000 provides that video surveillance according to para 4 is prohibited at locations that are part of the most personal area of life of a data subject (e.g. their homes in general and also changing rooms, bathrooms, etc.).

Furthermore, video surveillance for the purpose of control of employees at workplaces (efficiency control) is expressly prohibited.

This provision does not generally prevent the surveillance of workplaces (e.g. the surveillance of dangerous machines in order to protect the employees or the surveillance of e.g. the counter hall of a bank), as long as the purpose is not efficiency control or employee monitoring as such. In all cases of video surveillance of a workplace the works council will need to give its consent to such surveillance.

10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

If a works council is established in the respective entity, an agreement needs to be concluded with the works council. Individual consent of the employee does not suffice in this case. In case no works council is established, each employee needs to provide its consent to the respective video surveillance of its workplace (if such is not at all prohibited by section 50a para 5 DSG 2000).

10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

See question 10.3 above.

10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?

As set out above, "employee monitoring" as such is prohibited. In case of a surveillance of a workplace for other purposes as set out in question 10.2, the normal rules apply.

11 Processing Data in the Cloud

11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Currently, Austrian law contains no specific rules regarding cloud computing, i.e. the normal rules apply. The entity owning the cloud or providing the cloud services is regarded as the data processor because he acts solely on behalf of the respective data controller who has taken the decision to process the relevant data.

11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

According to section 11 para 2 DSG 2000, agreements between the data controller and the data processor need to be concluded in writing and must at least require the processor to:

- use data only according to the instructions of the data controller; in particular, the transmission of the data used is prohibited unless so instructed by the data controller;
- take all required safety measures in accordance with section 14 DSG 2000; in particular to employ only operatives who have committed themselves to confidentiality *vis-á-vis* the processor or are under a statutory obligation of confidentiality;
- enlist another processor only with the permission of the controller; insofar as this is possible given the nature of the service processing to create in agreement with the controller the necessary technical and organisational requirements for the fulfilment of the controller's obligation to grant the right of information, rectification and deletion;
- hand over to the controller after the end of the service processing all results of processing and documentation containing data or to keep or destroy them on his request; and
- make available to the controller all information necessary to control the compliance with the above obligations.

12 Big Data and Analytics

12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

There are now specific legal provisions in the law referring to big data and analytics, i.e. the normal rules apply. No guidance of the DSB has been issued in this respect so far.

13 Data Security and Data Breach

13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?

Section 14 DSG 2000 requires the data controller to adopt and implement adequate security measures in order to safeguard the protection of personal data (e.g. the allocation of competences within the respective entity regarding the use of data, limitation of access to the data controller's premises and to data and programmes. Protocol and documentation duties); however, neither the law nor guidance by the DSB defines any specific data security standards to be used.

13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Austrian data protection law does not contain a general obligation to notify data breaches with the DSB.

However, within the scope of the Telecommunications Act ("*Telekommunikationsgesetz 2003*" – TKG 2003, containing the implementation of Directive 2002/58 EC, as amended) the operator of a public communication service is required to notify any data breaches immediately with the Data Protection Authority.

13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.

Yes. The data controller is obliged to inform the data subject immediately:

- if data contained in one of his data applications has been subject to *severe and systematic unlawful use*; and
- such use could be *harmful* for the data subject (section 24a DSG 2000).

The law requires "immediate" notification but provides no further guidance regarding the timeframe or other details of the information or how the data subjects shall be informed.

The law obliges the data controller to decide whether a "severe and systematic unlawful use" is given which could be "harmful" for the data subject and finally in which way the data subject shall be informed about the data breach.

In principle, no voluntary reporting is expected.

14 Enforcement and Sanctions

14.1 Describe the enforcement powers of the data protection authority(ies):

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
According to section 30 DSG 2000, the DSB is, in case it suspects a violation of data controller's obligations *vis-à-vis* data subjects or in case of data applications subject to prior approval of the DSB, entitled to: ■ require any explanations by the data controller; ■ require the data controller to submit any documentation; and ■ examine data controller's compliance with its duties according to the DSG 2000, such as by investigating in the premises of the data controller. The DSB may subsequently: ■ Expressly prohibit the respective use of data/a data application. ■ Issue recommendations to the data controller. ■ Lodge a complaint with the respective criminal court or the respective regional administrative authority ("*Bezirksverwaltungs-behörde*").	Violation of the DSG 2000 can be sanctioned by an administrative fine of up to €25,000; the competent authority for the decision upon the fine is the respective regional administrative authority. "*Bezirksverwaltungsbehörde*". A data subject which claims that its data privacy rights have been violated by an individual or a private entity has the following civil remedies against the data controller: ■ Right to forbearance and removal. ■ Right to compensation for damages. The action has to be filed with the competent **Civil Regional Court**; a preliminary injunction also may be issued under facilitated conditions. If a data subject claims that its data privacy rights have been violated by a public entity, the **DSB** decides on such complaints. Generally, a complaint can be filed with the DSB if a data subject claims that its right to information has been violated.	The unlawful use of data e.g. by any data controller or data processor with the intention to enrich itself or a third party or to cause damage to third parties is a criminal offence punishable by imprisonment for up to one year (section 51 DSG 2000). The Competent Authority is the **Criminal (District) Court**. Please note that even only attempted data breaches may be punished; and further, any data carrier or programmes as well as picture transmitting or recording devices may be confiscated, if they are linked to an offence.

14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Regarding its enforcement powers according to section 30 DSG 2000, the most frequent action taken by the DSB seems to be the issuance of recommendations to the respective data controller in which the data controller is required to adopt and implement these recommendations within a certain period of time (up to several months, given the measures to be taken by the data controller). A common example is the case of "Google Street View", in which the DSB has in the first place required that Google Street View needed to be notified with the DSB and has further issued several recommendations to Google regarding the blurring of faces, number plates and pictures of private property.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within Austria respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

Austrian law does not contain an equivalent to discovery or e-discovery as known in US law. Foreign e-discovery requests will generally collide with data protection law, as the normal rules will apply as to whether it is permitted to transfer data a) to a third person, and b) to a country outside the EEA not providing for adequate data protection.

15.2 What guidance has the data protection authority(ies) issued?

The DSB has so far not issued any guidance in this respect.

Dr. Sonja Hebenstreit

Herbst Kinsky Rechtsanwälte GmbH
Dr. Karl Lueger Platz 5
A 1010 Vienna
Austria

Tel: *+43 1 904 2180 161*
Fax: *+43 1 904 2180 120*
Email: *sonja.hebenstreit@herbstkinsky.at*
URL: *www.herbstkinsky.at*

Dr. Sonja Hebenstreit was admitted to the Austrian Bar in 2003 and joined Herbst Kinsky Rechtsanwälte GmbH in 2005. She specialises in the fields of intellectual and industrial property law, unfair competition, pharmaceutical law, antitrust and competition law, as well as in data protection law.
Education and Career: *Mag. iur.* (Vienna 1997); *Dr. iur.* (Vienna 2001); internship with the European Commission (Brussels 1998); trainee at British Telecommunications Group Legal Services (Brussels 1999); researcher at the University of Münster, ITM/Civil Law Department (1999-2000); law practice with Hausmaninger Herbst Attorneys at Law (2000-2005) and Herbst Kinsky since 2005. Admitted to the Austrian Bar (Vienna 2003).
Languages: German, English and French.

Dr. Isabel Funk-Leisch

Herbst Kinsky Rechtsanwälte GmbH
Dr. Karl Lueger Platz 5
A 1010 Vienna
Austria

Tel: *+43 1 904 2180 152*
Fax: *+43 1 904 2180 120*
Email: *isabel.funk@herbstkinsky.at*
URL: *www.herbstkinsky.at*

Dr. Isabel Funk-Leisch joined Herbst Kinsky Rechtsanwälte GmbH in 2008. She specialises in the field of commercial law, as well as public law, pharmaceutical law and data protection law.
Education and Career: *Mag. iur.* (Vienna 2004); *Dr. iur.* (Vienna 2008); law practice as associate at a law firm in Vienna specialised in the field of commercial law; associate at Herbst Kinsky Rechtsanwälte GmbH in 2008; admitted to the Austrian Bar (Vienna 2010); publications on the law on insurance intermediation.
Languages: German, English and French.

HERBST KINSKY
RECHTSANWÄLTE GMBH

THE FIRM

Since its establishment in 2005, Herbst Kinsky has become one of Austria's leading commercial law firms. Its specialised and highly committed lawyers combine many years of experience, gained abroad and in reputable Austrian law firms. The firm's practice covers a full range of services in all areas of commercial, corporate, civil and public law, including banking, insurance and capital markets, corporate and M&A, IP, IT and life sciences, merger control, anti-trust and competition, real estate, dispute resolution and arbitration.

OUR CLIENTS

The firm's clients range from large international privately-held and publicly-listed companies, banks, insurance companies and private equity investors to small and mid-size business entities. Clients cut across many different industries, including energy, information technology, financial institutions, insurance, engineering, construction, pharmaceuticals and healthcare.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Environment & Climate Change Law
- Franchise
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Patents
- Pharmaceutical Advertising
- Private Client
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet

GLG
Global Legal Group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: sales@glgroup.co.uk

www.iclg.co.uk