ICLG

The International Comparative Legal Guide to:

Data Protection 2017

4th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bae, Kim & Lee LLC
Bagus Enrico & Partners
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Cuatrecasas
Dittmar & Indrenius
Drew & Napier LLC
Ecija Abogados
ErsoyBilgehan
Eversheds Sutherland
GANADO Advocates
Gilbert + Tobin
GRATA International
Hacohen & Co.
Herbst Kinsky Rechtsanwälte GmbH
Hunton & Williams
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
LPS L@w
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at Law Ltd.
Portolano Cavallo
Rato, Ling, Lei & Cortés Lawyers
Rossi Asociados
Subramaniam & Associates (SNA)
Wikborg Rein Advokatfirma AS

global legal group

global legal group

Contributing Editors
Anita Bapat and Aaron P. Simpson, Hunton & Williams

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Paul Mochalski

Sub Editor
Hollie Parker

Senior Editors
Suzie Levy, Rachel Williams

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

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 2017

ISBN 978-1-911367-50-5
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

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 the 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*" (hereinafter 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 for advising the Federal Government and the State Governments on requests concerning data protection law (section 41 para 2 DSG 2000).

2 Definitions

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 Personal Data concerns a particular category of data deserving special protection. Sensitive Personal 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 Personal 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**"

  The 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**"

  The 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 Subject**"

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

- *Other key definitions – please specify* (*e.g.,* "*Pseudonymous Data*", "*Direct Personal Data*", "*Indirect Personal Data*")

  - "**Indirect Personal Data**"

    Data are only "indirectly personal" for a Controller, a Processor or recipient of a transmission when the data relate to the Data Subject in such a manner that the Controller, Processor or recipient of a transmission cannot establish the identity of the Data Subject by legal means.

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' legitimate interest in secrecy 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 legitimate 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 number 5 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.

- *Other key principles – please specify*

  - **Data security**

    Any Data Controller or Data Processor needs to safeguard the security of the data it processes and is obliged to take appropriate measures to ensure data security shall be taken by all organisational units.

  - **Correctness and actuality**

    Data shall only be used in a way 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**

  According to section 26 para 1 DSG 2000, a Data Controller shall provide any person or group of persons with information regarding 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 cases where 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, along with the possibility to inspect and make duplicates or photocopies instead of being provided in writing.

  The information shall not be given if protecting the information 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, which 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 established requirements, 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 must 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 if there has been an infringement of its preponderant interest in secrecy deserving protection and 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. This is only applicable 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.

- *Other key rights – please specify*

  - **Compensation of damages**

    According to section 33 DSG 2000, a Data Controller or Data Processor who has culpably used data contrary to the provisions of the DSG 2000, shall indemnify the Data Subject pursuant to the general provisions of civil law. However, due to Austrian civil law, only material damages are covered by this general rule.

Solely in the event that sensitive data, data about the Data Subject's creditworthiness or data about (judicial or administrative) offences are publicly used in a way Data Subjects' interests in secrecy are violated, the Data Subject is entitled to claim indemnity for immaterial damage from the Data Processor for the insult suffered. The indemnity of immaterial damage must not exceed EUR 20,000.

The Data Controller or Data Processor shall also be liable for damage caused by their staff, insofar as their action was causal for the damage. They shall be free from liability if they can prove that the circumstances which caused the damage cannot be attributed to him or his staff.

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);
- concerns the management of registers and catalogues that are by law open to access by the public;
- contains only Indirect Personal Data;
- is carried out by natural persons for entirely private reasons; or
- concerns solely 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, 37 standard applications have been defined for different purposes of private and public Data Controllers, all of which list exactly 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, as amended by Federal Law Gazette II No. 278/2015.

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 to and who are therefore regarded as Data Controllers according to DSG 2000 also have to be listed in the notification.

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 use the web application directly; 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 about:

- the purpose of the data application;
- 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;
- any reasons for the deletion of a data application; and
- the existence of the appropriate legal basis for the registration of the data application.

According to section 9 DVRV 2012, the information for a new registration or a change of registration regarding a data application must be filled out on the online document of the respective "appendix 2" formula (notification of a data application).

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

The notification duties are set out in section 17 DSG 2000. A failure to register/notify is deemed as an administrative offence and is punishable by a fine of up to EUR 10,000, 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 up to date. Changes and modifications to data applications which have already been 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 of 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 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, Uruguay and New Zealand) does not require authorisation.

The EU-US Privacy Shield provides similar possibilities to transmit and commit data to the USA for registered companies without approval by the DSB.

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

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

According to section 52 DSG 2000, fines may be imposed 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 (for example) sensitive data, i.e., no separate application is required in such a case.

A cross-border data exchange is not exempt from authorisation according to section 12 DSG 2000, as the Controller has to (separately) apply for approval from the DSB prior to transmitting or committing the data (section 13 para 1 DSG 2000). The DSB can issue the approval subject to conditions and stipulations.

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 of data outlined in the application for the permit in the 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 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 cross-border 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 in practice last from two 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 a 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 compliance with regard to the use of Personal Data and the fulfilment of legal requirements. The appointment of a Data Protection Officer provides no direct legal advantages under Austrian law. However, it might be – depending on the size and structure of an undertaking – most useful for an

undertaking to designate a Data Protection Officer and provide him with the respective tasks and competences in order to safeguard the undertaking's compliance with data protection 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 the following:

- supervision and control of compliance with the legal and internal requirements regarding the use of Personal Data;
- DSB notification requirements; and
- 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 cases of reasonable suspicion of an 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, email, 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 email or SMS marketing activities.

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 when somebody makes a complaint.

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 Are companies required to screen against any "do not contact" list or registry?

In the case of email and SMS-marketing without the recipient's prior consent, the "Robinson List" needs to be checked.

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

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

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 EUR 58,000.

7.5 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 2000. 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) published a Working Document 02/2013 (WP 208) 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 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, section 96 para 3 TKG and the necessary consent.

7.6 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 7.5.

7.7 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.

7.8 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 EUR 37,000.

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 EEA. Furthermore, transfer of data to a recipient outside the EEA 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 (in principle) to EU-US Privacy Shield 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 the Data Subject and the 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 (in principle, within a shorter period of time; see also 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 an EU-US Privacy Shield 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 two and 36 months (see also 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-blowing systems, but the DSB has rendered several decisions on the installation of whistle-blowing systems. As the subject of a report of employees through whistle-blowing 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 in the past approved the use of data in the context of a whistle-blowing 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 a 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;
- any Personal Data obtained by means of the whistle-blowing system must be deleted within two months after the completion of the respective inquiry;

- only data concerning executive employees and similar responsible employees ("*leitende Angestellte und vergleichbar verantwortliche Personen*") who are accused of severe misconduct may be transferred to a foreign holding company of the Data Controller; and
- the Data Controller has concluded a contract with the service provider of the system in order to ensure that only contents approved by the DSB are transferred to the foreign holding company.

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

For specific whistle-blower systems of credit institutions, a standard application (SA 036) has been established.

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 the DSB's approval has in the past been several years.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

Yes, insofar as the whistle-blower who decides to disclose his data (in particular his name) needs to be informed on the use of that data.

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

An agreement with the works council is required for the implementation of a whistle-blowing system. The DSB has in the past required that such works council agreement be provided to the authority or has granted approval only under the condition that a works council agreement is concluded.

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 cases where 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 cases where 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 analogue video recording system.

The Controller of a video surveillance system is obliged to put up appropriate signs in order to inform the Data Subjects about the video surveillance.

The DSG 2000 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 a way, are only 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 of 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 cases where the video surveillance is not made in the performance of official executive tasks (i.e., for private purposes), it does not infringe the interests of 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 undertake 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 the transfer of data recorded by video surveillance:

- to the competent authority or the court, if the Controller has reasonable grounds 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 deemed to be part of the most personal area of the Data Subject's life (e.g., their homes in general and also changing rooms, bathrooms, etc.).

Furthermore, video surveillance for the purpose of control of employees in the workplace (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 cases where no works council is established, each employee needs to provide its consent to the respective video surveillance of its workplace (if such is not 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?

Please 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 the case of 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 it 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-à-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 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 no 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 so far in this respect.

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 the data applications; protocol and documentation duties); however, neither the law nor guidance of 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 to 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 to 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" has occurred, whether it could be "harmful" to 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.

13.4 What are the maximum penalties for security breaches?

Anyone who grossly neglects the required data security measures according to section 14 DSG 2000 commits an administrative offence punishable by a fine of up to EUR 10,000.

In cases where a data breach is carried out by someone with the intention to enrich himself or a third person unlawfully or with the intention to harm someone in his right guaranteed according to section 1 para 1 DSG 2000, such behaviour might be subject to a court punishment of imprisonment for up to one year.

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 cases where it suspects a violation of a Data Controller's obligations *vis-à-vis* Data Subjects or in cases of data applications subject to prior approval of the DSB, entitled to: ■ require an explanation from the Data Controller; ■ require the Data Controller to submit any documentation; and ■ examine the Data Controller's compliance with its duties according to the DSG 2000, for example, by investigating the premises of the Data Controller. The DSB may subsequently: ■ Expressly prohibit the respective use of data or a data application. ■ Issue recommendations to the Data Controller. Lodge a complaint with the respective criminal court or the respective regional administrative authority ("*Bezirksverwaltungsbehörde*").	Violation of the DSG 2000 can be sanctioned by an administrative fine of up to EUR 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 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, depending on 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 instance required that Google Street View needs to be registered with the DSB and has further issued several recommendations to Google regarding the blurring of faces, number plates and pictures of private property.

Furthermore, the DSB carries out "sector investigations" in order to check whether compliance with data protection laws is given in a specific industry or institutions. Past sector investigations have focused on hospitals and credit report agencies.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

15.1 How do companies within your jurisdiction 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 which does not provide 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.

16 Trends and Developments

16.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

The Administrative High Court has ruled that "Dash Cams" (for the purpose of preservation of evidence in the event of traffic accidents) are prohibited if the user could save the video at any time. In the particular case (Ro 2015/04/0011), the "Dash Cam" erased the video about a minute after recording, if a strong collision (e.g. an accident) was detected; furthermore, the video could be saved by pressing a "SOS" button. The Administrative High Court qualified this as unlawful CCTV.

However, the Administrative High Court did not rule that "Dash Cams" are prohibited in general; it can be expected that "Dash Cams" without the possibility for the user to save the video at any time are compatible with Austrian data protection law.

16.2 What "hot topics" are currently a focus for the data protection regulator?

The most important topic is the General Data Protection Regulation (hereinafter referred to as "GDPR") and its "implementation" into Austrian law, as some opening/flexibility clauses in the GDPR require national implementation acts. However, the Austrian authorities have not yet published any proposals for such legislation.

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 210*
Email: *sonja.hebenstreit@herbstkinsky.at*
URL: *www.herbstkinsky.at*

Dr. Sonja Hebenstreit is a partner of Herbst Kinsky Rechtsanwälte GmbH, which she joined 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 Rechtsanwälte GmbH since 2005; and 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 210*
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 an 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); and has publications on the law on insurance intermediation.

Languages: German; English; and French.

HERBST KINSKY
RECHTSANWÄLTE GMBH

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, antitrust 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 Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

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

www.iclg.com