ICLG

The International Comparative Legal Guide to:

Data Protection 2018

5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Anderson Mōri & Tomotsune
Ashurst Hong Kong
BSA Ahmad Bin Hezeem & Associates LLP
Clyde & Co
Cuatrecasas
DQ Advocates Limited
Ecija Abogados
Fırat İzgi Attorney Partnership
GANADO Advocates
GÖRG Partnerschaft von Rechtsanwälten mbB
Herbst Kinsky Rechtsanwälte GmbH
Holding Redlich
Jackson, Etti & Edu
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
KPMG Law Firm
Lee & Ko
Loyens & Loeff Luxembourg S.à r.l.
Loyens & Loeff N.V.
LPS L@w
Lydian
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
OLIVARES
OrionW LLC
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi Attorneys at law
Pillsbury Winthrop Shaw Pittman LLP
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Subramaniam & Associates (SNA)
Trevisan & Cuonzo Avvocati
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg
global legal group

global legal group

Contributing Editors
Tim Hickman & Dr. Detlev Gabel, White & Case LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Executive 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
June 2018

ISBN 978-1-912509-15-7
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

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

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?

From 25 May 2018, the principal data protection legislation in the EU will be Regulation (EU) 2016/679 (the "General Data Protection Regulation" or "GDPR"). The GDPR repeals Directive 95/46/EC (the "Data Protection Directive") and leads to increased (though not total) harmonisation of data protection law across the EU Member States.

The Data Protection Act Adaptation Act 2018 ("*Datenschutzgesetz-Anpassungsgesetz 2018*") Federal Law Gazette ("*Bundesgesetzblatt*" – "BGBl") I Nr. 120/2017 amends the current Data Protection Act 2000 ("*Datenschutzgesetz 2000*") in accordance with the GDPR and will enter into force on 25 May 2018 as the Austrian Data Protection Act ("*Datenschutzgesetz*", hereinafter "DSG"). Furthermore, Directive (EU) 2016/680 *on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA* is implemented into Austrian law by the Data Protection Act Adaptation Act 2018.

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

Data protection is impacted by labour law. The DSG 2000 did not contain a systematic regulation of data protection in the context of employment, but 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 processing activities, the consent of the works council is mandatory (please see questions in section 14).

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 authority(ies) are responsible for data protection?

The "*Datenschutzbehörde*" (hereinafter "DSB") is the national independent supervisory authority in Austria (see section 18 para 1 DSG).

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 14 *et seq.* DSG).

Until 24 May 2018, Austrian data protection law requires the registration of data applications with the DSB. This data processing register ("*Datenverarbeitungsregister*") will be continued for archiving purposes until 31 December 2019.

2 Definitions

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

- "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "**Processing**" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- "**Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- "**Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- "**Data Subject**" means an individual who is the subject of the relevant personal data.
- "**Sensitive Personal Data**" (or "Special Categories Of Personal Data") are personal data revealing racial or ethnic

origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life and sexual orientation, genetic data or biometric data.

- "**Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The GDPR applies to businesses that are established in any EU Member State, and that process personal data (either as a controller or processor, and regardless of whether or not the processing takes place in the EU) in the context of that establishment.

A business that is not established in any Member State, but is subject to the laws of a Member State by virtue of public international law is also subject to the GDPR.

The GDPR applies to businesses outside the EU if they (either as controller or processor) process the personal data of EU residents in relation to: (i) the offering of goods or services (whether or not in return for payment) to EU residents; or (ii) the monitoring of the behaviour of EU residents (to the extent that such behaviour takes place in the EU).

Further, the GDPR applies to businesses established outside the EU if they monitor the behaviour of EU residents (to the extent such behaviour takes place in the EU).

4 Key Principles

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

- **Transparency**

  Personal data must be processed lawfully, fairly and in a transparent manner. Controllers must provide certain minimum information to data subjects regarding the collection and further processing of their personal data. Such information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

- **Lawful basis for processing**

  Processing of personal data is lawful only if, and to the extent that, it is permitted under EU data protection law. The GDPR provides an exhaustive list of legal bases on which personal data may be processed, of which the following are the most relevant for businesses: (i) prior, freely given, specific, informed and unambiguous consent of the data subject; (ii) contractual necessity (i.e., the processing is necessary for the performance of a contract to which the data subject is a party, or for the purposes of pre-contractual measures taken at the data subject's request); (iii) compliance with legal obligations (i.e., the controller has a legal obligation, under the laws of the EU or an EU Member State, to perform the relevant processing); or (iv) legitimate interests (i.e., the processing is necessary for the purposes of legitimate interests pursued by the controller, except where the controller's interest are overridden by the interests, fundamental rights or freedoms of the affected data subjects).

  Please note that businesses require stronger grounds to process sensitive personal data. The processing of sensitive personal data is only permitted under certain conditions, of which the most relevant for businesses are: (i) explicit consent of the affected data subject; (ii) the processing is necessary in the context of employment law; or (iii) the processing is necessary for the establishment, exercise or defence of legal claims.

- **Purpose limitation**

  Personal data may only be collected for specified, explicit and legitimate purposes and must not be further processed in a manner that is incompatible with those purposes. If a controller wishes to use the relevant personal data in a manner that is incompatible with the purposes for which they were initially collected, it must: (i) inform the data subject of such new processing; and (ii) be able to rely on a lawful basis as set out above.

- **Data minimisation**

  Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed. A business should only process the personal data that it actually needs to process in order to achieve its processing purposes.

- **Accuracy**

  Personal data must be accurate and, where necessary, kept up to date. A business must take every reasonable step to ensure that personal data that are inaccurate are either erased or rectified without delay.

- **Retention**

  Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

- **Data security**

  Personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

- **Accountability**

  The controller is responsible for, and must be able to demonstrate, compliance with the data protection principles set out above.

5 Individual Rights

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

- **Right of access to data/copies of data**

  A data subject has the right to obtain from a controller the following information in respect of the data subject's personal data: (i) confirmation of whether, and where, the controller is processing the data subject's personal data; (ii) information about the purposes of the processing; (iii) information about the categories of data being processed; (iv) information about the categories of recipients with whom the data may be shared; (v) information about the period for which the data will be stored (or the criteria used to be determine that period); (vi) information about the existence of the rights to erasure, to rectification, to restriction of processing and to object to processing; (vii) information about the existence of the right to complain to the relevant data protection authority; (viii) where the data were not collected from the data subject, information as to the source of the data; and (ix) information about the existence of, and an explanation of the logic involved in, any automated processing that has a significant effect on the data subject.

Additionally, the data subject may request a copy of the personal data being processed.

- **Right to rectification of errors**

  Controllers must ensure that inaccurate or incomplete data are erased or rectified. Data subjects have the right to rectification of inaccurate personal data.

- **Right to deletion/right to be forgotten**

  Data subjects have the right to erasure of their personal data (the "right to be forgotten") if: (i) the data are no longer needed for their original purpose (and no new lawful purpose exists); (ii) the lawful basis for the processing is the data subject's consent, the data subject withdraws that consent, and no other lawful ground exists; (iii) the data subject exercises the right to object, and the controller has no overriding grounds for continuing the processing; (iv) the data have been processed unlawfully; or (v) erasure is necessary for compliance with EU law or national data protection law.

- **Right to object to processing**

  Data subjects have the right to object, on grounds relating to their particular situation, to the processing of personal data where the basis for that processing is either public interest or legitimate interest of the controller. The controller must cease such processing unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the relevant data subject or requires the data in order to establish, exercise or defend legal rights.

- **Right to restrict processing**

  Data subjects have the right to restrict the processing of personal data, which means that the data may only be held by the controller, and may only be used for limited purposes if: (i) the accuracy of the data is contested (and only for as long as it takes to verify that accuracy); (ii) the processing is unlawful and the data subject requests restriction (as opposed to exercising the right to erasure); (iii) the controller no longer needs the data for their original purpose, but the data are still required by the controller to establish, exercise or defend legal rights; or (iv) verification of overriding grounds is pending, in the context of an erasure request.

- **Right to data portability**

  Data subjects have a right to receive a copy of their personal data in a commonly used machine-readable format, and transfer their personal data from one controller to another or have the data transmitted directly between controllers.

- **Right to withdraw consent**

  A data subject has the right to withdraw their consent at any time. The withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject must be informed of the right to withdraw consent. It must be as easy to withdraw consent as to give it.

- **Right to object to marketing**

  Data subjects have the right to object to the processing of personal data for the purpose of direct marketing, including profiling.

- **Right to complain to the relevant data protection authority(ies)**

  Data subjects have the right to lodge complaints concerning the processing of their personal data with the data protection authority in Austria, if the data subjects lives in Austria or the alleged infringement occurred in Austria.

- **Right to basic information**

  Data subjects have the right to be provided with information on the identity of the controller, the reasons for processing their personal data and other relevant information necessary to ensure the fair and transparent processing of personal data.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Until 24 May 2018, every processing activity required prior notification to the DSB (and in some cases even prior approval), unless a legal exception applied. As from 25 May 2018, the DSG no longer contains any such general notification obligations.

However, the DSG provides in its sections 7 and 8 for specific requirements for prior approval of the DSB (a) in the context of data processing in the public interest for the purposes of archiving, scientific or historical research or statistics, and (b) in the context of processing address data of data subjects for purposes of an important public interest regarding the notification or interview of that subjects.

The data processing register will be continued for archiving purposes until 31 December 2019.

The DSB has stated in its official guideline to the GDPR that all documentation to be provided to the DSB in the course of an (examination) proceeding (e.g., processing register, data protection impact assessment ("DPIA")) needs to be in German.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

Please see question 6.1 above.

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

Please see question 6.1 above.

6.4 Who must register with/notify the data protection authority (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)?

Please see question 6.1 above.

6.5 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)?

Please see question 6.1 above.

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

Please see question 6.1 above.

6.7 What is the fee per registration/notification (if applicable)?

Please see question 6.1 above.

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

Please see question 6.1 above.

6.9 Is any prior approval required from the data protection regulator?

Please see question 6.1 above.

6.10 Can the registration/notification be completed online?

Please see question 6.1 above.

6.11 Is there a publicly available list of completed registrations/notifications?

Please see question 6.1 above.

6.12 How long does a typical registration/notification process take?

Please see question 6.1 above.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a Data Protection Officer for controllers or processors is only mandatory in some circumstances including where there is: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

Where a business designates a Data Protection Officer voluntarily, the requirements of the GDPR apply as though the appointment were mandatory.

Austria has not made use of the possibility offered in Article 37 para 4 GDPR and has not provided for any further mandatory Data Protection Officer designation requirement.

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

In the circumstances where appointment of a Data Protection Officer is mandatory, failure to comply may result in the wide range of penalties available under the GDPR. In particular, it is subject to an administrative fine of the higher of up to 10 Mio EUR or 2% of the annual turnover of the respective controller according to Article 83 para 4 GDPR.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect to his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing their tasks and should report directly to the highest management level of the controller or processor.

In accordance with section 5 DSG, the Data Protection Officer is bound by secrecy towards in particular the identity of any persons who have contacted the Data Protection Officer. In case the respective data subject has a privilege to refuse to give legal evidence, and has made use of such privilege, the Data Protection Officer may not provide any information regarding the respective data.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

A single Data Protection Officer is permitted by a group of undertakings provided that the Data Protection Officer is easily accessible from each establishment.

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

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices. While this is not strictly defined, it is clear that the level of expertise required will depend on the circumstances. For example, the involvement of large volumes of sensitive personal data will require a higher level of knowledge.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

A Data Protection Officer should be involved in all issues which relate to the protection of personal data. The GDPR outlines the minimum tasks required by the Data Protection Officer which include: (i) informing the controller, processor and their relevant employees who process data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the processing of personal data including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data processing.

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

Yes, the controller or processor must notify the data protection authority of the contact details of the designated Data Protection Officer.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The Data Protection Officer does not necessarily need to be named in the public-facing privacy notice. However, the contact details of the Data Protection Officer must be notified to the data subject

when personal data relating to that data subject are collected. As a matter of good practice, the Article 29 Working Party ("WP29") recommends that both the data protection authority and employees should be notified of the name and contact details of the Data Protection Officer.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

Yes. The business that appoints a processor to process personal data on its behalf is required to enter into a written agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing and the obligations and rights of the controller (i.e., the business).

It is essential that the processor appointed by the business complies with the GDPR.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

The processor must be appointed under a binding agreement in writing. The contractual terms must stipulate that the processor: (i) only acts on the documented instructions of the controller; (ii) imposes confidentiality obligations on all employees; (iii) ensures the security of personal data that it processes; (iv) abides by the rules regarding the appointment of sub-processors; (v) implements measures to assist the controller with guaranteeing the rights of data subjects; (vi) assists the controller in obtaining approval from the Data Protection Officer; (vii) either returns or destroys the personal data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the controller with all information necessary to demonstrate compliance with the GDPR.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing. (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?)

According to section 107 para 2 Austrian Telecommunications Act ("*Telekommunikationsgesetz 2003*", containing the implementation of Directive 2002/58 EC, as amended; hereinafter "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 Austrian E-Commerce Act).

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

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

According to section 107 para 1 TKG, marketing by telephone, 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. For marketing by post, no restrictions (as applicable for calls or emails) apply.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

If unlawful direct marketing actions have not been committed in Austria, they shall be considered as having been committed in the place where the call reaches the subscriber's line. As a result, this means that any direct marketing action is judged according to the aforementioned rules when the message/call was received in Austria. However, it is often not possible for the authority to prosecute legal violations abroad.

9.4 Is/are 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 data protection authority is not responsible for the enforcement of such violations. The authority mainly becomes active when somebody makes a complaint.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

Undertakings holding a licence under section 151 Austrian Trade Act ("*Gewerbeordnung*") are entitled to collect data from publicly available sources (and to add classifications for specific marketing purposes) for the preparation and execution of marketing purposes for third parties and are entitled to sell such lists to third parties. The purchase of such lists will therefore be admissible. However, when using purchased marketing lists from third parties for the purpose of sending any electronic communication, it needs to be safeguarded that the recipient of the advertising has indeed given consent for electronic direct marketing.

9.6 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.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

Section 96 para 3 TKG implements Article 5 of the ePrivacy Directive. Pursuant to Article 5 of the EU ePrivacy Directive, the storage of cookies (or other data) on an end user's device requires prior consent (the applicable standard of consent is derived from Directive 95/46/EC and, from 25 May 2018, the GDPR). For consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual's wishes. This does not apply if: (i) the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (ii) the cookie is strictly necessary to provide an "information society service" (e.g., a service over the internet) requested by the subscriber or user, which means that it must be essential to fulfil their request.

10.2 The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The regulation is planned to come into force May 25, 2018 and will provide amended requirements for the usage of cookies. Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The WP29 published a Working Document 02/2013 (WP 208) providing guidance on obtaining consent for cookies. Following WP29, the consent to the use of cookies containing personal data has to be explicit opt-in consent. The opinion of WP29 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.

However, section 93 para 3 TKG does not distinguish between different types of cookies.

10.3 To date, has/have 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.

10.4 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.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Data transfers to other jurisdictions that are not within the European Economic Area (the "EEA") can only take place if the transfer is to an "Adequate Jurisdiction" (as specified by the EU Commission) or the business has implemented one of the required safeguards as specified by the GDPR.

11.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

When transferring personal data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR. The GDPR offers a number of ways to ensure compliance for international data transfers, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or Binding Corporate Rules ("BCRs").

Businesses can adopt the Standard Contractual Clauses drafted by the EU Commission – these are available for transfers between controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place on the basis of contracts agreed between the data exporter and data importer provided that they conform to the protections outlined in the GDPR, and they have prior approval by the relevant data protection authority.

International data transfers within a group of businesses can be safeguarded by the implementation of BCRs. The BCRs will always need approval from the relevant data protection authority. Most importantly, the BCRs will need to include a mechanism to ensure they are legally binding and enforced by every member in the group of businesses. Among other things, the BCRs must set out the group structure of the businesses, the proposed data transfers and their purpose, the rights of data subjects, the mechanisms that will be implemented to ensure compliance with the GDPR and the relevant complainant procedures.

Transfer of personal data to the US is also possible if the data importer has signed up to the EU-US Privacy Shield Framework, which was designed by the US Department of Commerce and the EU Commission to provide businesses in the EU and the US with a mechanism to comply with data protection requirement when transferring personal data from the EU to the US.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

It is likely that the international data transfer will require prior approval from the relevant data protection authority unless they have already established a GDPR-compliant mechanism as set out above for such transfers.

In any case, most of the safeguards outlined in the GDPR will need initial approval from the data protection authority, such as the establishment of BCRs.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Internal whistle-blowing schemes are generally established in pursuance of a concern to implement proper corporate governance principles in the daily functioning of businesses. Whistle-blowing is designed as an additional mechanism for employees to report misconduct internally through a specific channel and supplements a business' regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconducts.

The WP29 has limited its Opinion 1/2006 on the application of EU data protection rules to internal whistle-blowing schemes to the fields of accounting, internal accounting controls, auditing matters, the fight against bribery, banking and financial crime. The scope of corporate whistle-blower hotlines, however, does not need to be limited to any particular issues. The WP29 recommends that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

Article 10 GDPR requires that the processing of personal data relating to criminal convictions and offences shall only be carried out under the control of official authority or when the processing is authorised by EU or a Member State's law. In Austria, this would currently be given for whistle-blower hotlines of financial institutions according to section 99g Banking Act ("*Bankwesengesetz*").

12.2 Is anonymous reporting prohibited, or strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited under EU data protection law; however, it raises problems as regards the essential requirement that personal data should only be collected fairly. As a rule, the WP29 considers that only identified reports should be advertised in order to satisfy this requirement. Businesses should not encourage or advertise the fact that anonymous reports may be made through a whistle-blower scheme.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer due to his/her action. The whistle-blower, at the time of establishing the first contact with the scheme, should be informed that his/her identity will be kept confidential at all the stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or to the employee's line management. If, despite this information, the person reporting to the scheme still wants to remain anonymous, the report will be accepted into the scheme. Whistle-blowers should be informed that their identity may need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated as a result of any enquiry conducted by the whistle-blowing scheme.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The use of CCTV is allowed if made in accordance with sections 12, 13 DSG. In such case, no DPIA must be undertaken in line with Article 35 para 10 GDPR. Sections 12 and 13 DSG have been enacted in accordance with Article 6 para 2 and 3, Article 23 and chapter IX GDPR and following the experiences made with the rules on CCTV that were contained in the DSG 2000.

In principle, CCTV is allowed if:

- it is required in the vital interest of a person;
- the data subject has consented to the use of its data;
- it is allowed by specific legal provisions; or
- in case of preponderant legal interests of the controller or a third person, provided that the processing is proportionate.

Section 12 para 3 DSG 2000 specifies that preponderant legal interests are given in case the CCTV is made for purposes of:

- the precautionary protection of persons or things on private property that is used only by the controller;
- the precautionary protection of persons or things on publicly accessible property being under the domestic authority of the controller, in case violations have already been happened in the past or there is a specific potential danger; or
- a private documentation interest in case the CCTV is neither directed to capture uninvolved persons, in a way allowing their identification nor to capture objects which would indirectly allow the identification of such persons.

CCTV in principle needs to be specifically marked by a sign which identifies the respective controller (section 13 para 4 DSG).

The DSB has stated in its draft White List for the DPIA that specific CCTV processing (as defined in the White List) does not require a DPIA.

13.2 Are there limits on the purposes for which CCTV data may be used?

According to section 12 para 4 DSG, CCTV is not permitted for the purpose of (i) control of employees in the workplace (please see question 14.1 below), (ii) automation-supported comparison of personal data obtained by means of CCTV with other personal data, and (iii) the evaluation of personal data obtained by means of CCTV on the basis of special categories of personal data (Article 9 GDPR) as a selection criterion.

Section 13 para 3 provides that any recordings need to be deleted if they are no longer required for the purpose for which they were collected, unless another legal obligation applies. In any case, the storing of recordings exceeding 72 hours needs to be proportionate and needs to be separately documented and justified.

14 Employee Monitoring

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

Section 12 para 4 number 1 DSG provides that CCTV 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.) without explicit consent.

Furthermore, CCTV for the purpose of control of employees in the workplace (efficiency control) is expressly prohibited (section 12 para 4 number 2 DSG).

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 most cases of video surveillance of a workplace, the works council will need to give its consent to such surveillance. Furthermore, please refer to the answers to section 13 above.

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

Pursuant to section 13 para 4 DSG, CCTV must be marked appropriately.

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 already prohibited by section 12 para 4 number 2 DSG).

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

Please see question 14.2 above.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes. Personal data must be processed in a way which ensures security and safeguards against unauthorised or unlawful processing, accidental loss, destruction and damage of the data.

Both controllers and processors must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk this may include the encryption of personal data, the ability to ensure the ongoing confidentiality, integrity and resilience of processing systems, an ability to restore access to data following a technical or physical incident and a process for regularly testing and evaluating the technical and organisation measures for ensuring the security of processing.

15.2 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) expect(s) voluntary breach reporting.

The controller is responsible for reporting a personal data breach without undue delay (and in any case within 72 hours of first becoming aware of the breach) to the relevant data protection authority, unless the breach is unlikely to result in a risk to the rights and freedoms of the data subject(s). A processor must notify any data breach to the controller without undue delay.

The notification must include the nature of the personal data breach including the categories and number of data subjects concerned, the name and contact details of the Data Protection Officer or relevant point of contact, the likely consequences of the breach and the measures taken to address the breach including attempts to mitigate possible adverse effects.

15.3 Is there a legal requirement to report data breaches to affected data subjects? 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) expect(s) voluntary breach reporting.

Controllers have a legal requirement to communicate the breach to the data subject, without undue delay, if the breach is likely to result in a high risk to the rights and freedoms of the data subject.

The notification must include the name and contact details of the Data Protection Officer (or point of contact), the likely consequences of the breach and any measures taken to remedy or mitigate the breach.

The controller may be exempt from notifying the data subject if the risk of harm is remote (e.g., because the affected data is encrypted), the controller has taken measures to minimise the risk of harm (e.g., suspending affected accounts) or the notification requires a disproportionate effort (e.g., a public notice of the breach).

15.4 What are the maximum penalties for data security breaches?

The maximum penalty is the higher of EUR 20 million or 4% of worldwide turnover.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
Investigative Powers	The data protection authority has wide powers to order the controller and the processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the controller or processor of alleged infringement of the GDPR, to access all personal data and all information necessary for the performance of controllers' or processors' tasks and access to the premises of the data including any data processing equipment.	N/A

Investigatory Powers	Civil/Administrative Sanction	Criminal Sanction
Corrective Powers	The data protection authority has a wide range of powers including to issue warnings or reprimands for non-compliance, to order the controller to disclose a personal data breach to the data subject, to impose a permanent or temporary ban on processing, to withdraw a certification and to impose an administrative fine (as below). 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 (section 62 DSG).	The unlawful use of data 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 or a fine of up to 720 daily rates (section 63 DSG). The Competent Authority is the Criminal (District) Court.
Authorisation and Advisory Powers	The data protection authority has a wide range of powers to advise the controller, accredit certification bodies and to authorise certificates, contractual clauses, administrative arrangements and binding corporate rules as outlined in the GDPR.	N/A
Imposition of Administrative Fines for Infringements of Specified GDPR Provisions	The GDPR provides for administrative fines which can be EUR 20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year. The DSG contains further administrative fines – subsidiary to the GDPR fines – of up to EUR 50,000.	N/A
Non-Compliance With a Data Protection Authority	The GDPR provides for administrative fines which will be EUR 20 million or up to 4% of the business' worldwide annual turnover of the proceeding financial year, whichever is higher.	N/A

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

The GDPR entitles the relevant data protection authority – in Austria the DSB – to impose a temporary or definitive limitation including a ban on processing. Such ban can be imposed by the DSB by rendering a decision ("*Bescheid*"); no court order is required.

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

Because the GDPR has not come into force (at the time of writing these replies), the data protection authority's approach to exercising those powers may not be described yet.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

Please see question 16.3 above.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do companies typically 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.

17.2 What guidance has/have the data protection authority(ies) issued?

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

18 Trends and Developments

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

In 2017, one of DSB's focuses was on public hospitals. The reviews showed that the healthcare providers largely complied with the provisions of the data protection laws; however, the DSB has issued recommendations to the hospitals.

Furthermore, DSB has provided guidance regarding the GDPR throughout 2017 and continues this activity in 2018. One major activity of the DSB this year will most likely consist of measures in the context of the GDPR getting into force on 25 May 2018.

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

Austria has already enacted an "implementation act" to the GDPR. Further national laws in the context of the GDPR (including a law slightly amending the Data Protection Adaptation Act) are in the legislative process and will probably be published in the Federal Gazzette in May 2018.

The amended section 11 DSG (not yet in force) explicitly states that the DSB shall, in line with Article 58 GDPR, in case of a first infringement of the GDPR, use its corrective powers in particular by issuing warnings.

The most important topic for the DSB is the GDPR and the changed legal framework. The DSB has published a guidance document in 2018 (available only in German) in which certain aspects of the GDPR are commented. In particular, the DSB has published a draft regulation regarding processing activities not requiring a DPIA ("white list"). A (draft) "black list" has not been issued so far.

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. 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 commercial law, public law, pharmaceutical law, data protection law as well as in the field of insurance intermediation.

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; and associate at Herbst Kinsky Rechtsanwälte GmbH in 2008. Admitted to the Austrian Bar (Vienna 2010).

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, antitrust and competition, data protection, 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
- Anti-Money Laundering
- 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
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State 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 Investment Funds
- 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