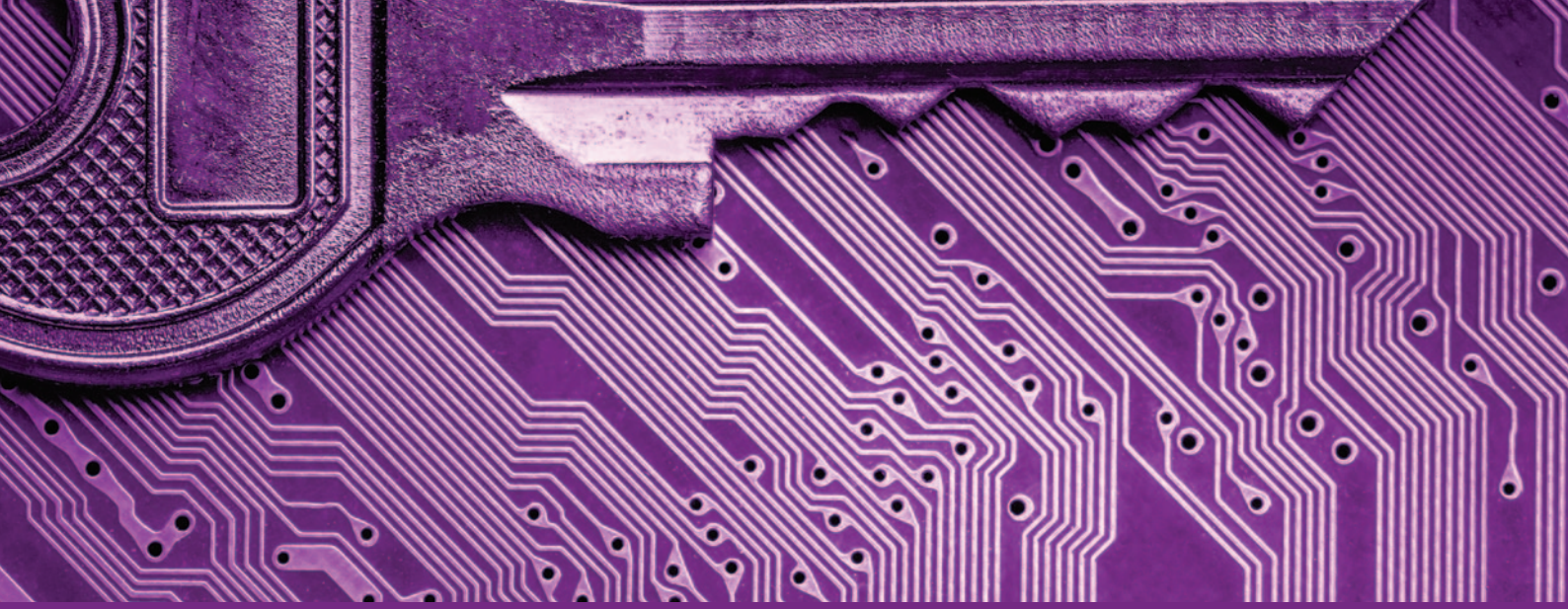

ICLG

The International Comparative Legal Guide to:

Data Protection 2019

6th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Ashurst Hong Kong
Assegaf Hamzah & Partners
BEITEN BURKHARDT
Bird & Bird
Christopher & Lee Ong
Çiğdemtekin Çakırca Arancı Law Firm
Clyde & Co
Cuatrecasas
Deloitte Legal Shpk
DQ Advocates Limited
Drew & Napier LLC
Ecija Abogados
FABIAN PRIVACY LEGAL GmbH
GANADO Advocates
Herbst Kinsky Rechtsanwälte GmbH
Herzog Fox & Neeman
Infusion Lawyers
Integra Law Firm
KADRI LEGAL
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys At Law
Lee & Ko
LPS L@w
Lydian
Matheson
Mori Hamada & Matsumoto
Morri Rossetti e Associati Studio Legale e Tributario
Nyman Gibson Miralis
OLIVARES
Osler, Hoskin & Harcourt LLP
Pestalozzi Attorneys at Law
Rato, Ling, Lei & Cortés – Advogados
Rossi Asociados
Rothwell Figg
S. U. Khan Associates Corporate & Legal Consultants
Subramaniam & Associates (SNA)
thg IP/ICT
Vaz E Dias Advogados & Associados
White & Case LLP
Wikborg Rein Advokatfirma AS

glg global legal group

global legal group

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

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Nicholas Catlin

Senior Editors
Caroline Collingwood
Rachel Williams

CEO
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 2019

ISBN 978-1-912509-76-8
ISSN 2054-3786

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

Continued Overleaf

global legal group

Country Question and Answer Chapters:

Austria

Herbst Kinsky Rechtsanwälte GmbH

Dr. Sonja Hebenstreit

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

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 The GDPR repealed Directive 95/46/EC ("Data Protection Directive") and leads to an increased (though not total) harmonisation of data protection law across the EU Member States.

The Data Protection Act Adaptation Act 2018 (*Datenschutzgesetz-Anpassungsgesetz 2018*), published in the Federal Law Gazette (*Bundesgesetzblatt* – "BGBl.") I Nr. 120/2017, amended the former Data Protection Act 2000 (*Datenschutzgesetz 2000*) in accordance with the GDPR and entered into force on 25 May 2018 as the Austrian Data Protection Act (*Datenschutzgesetz* – "DSG", as last amended by BGBl. 1 Nr. 14/2019). 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, was implemented into Austrian law by the Data Protection Act Adaptation Act 2018.

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

Labour law has a significant impact on data protection. As the DSG does not contain a systematic regulation of data protection in the context of employment, the principal legislation on data protection in this context is the Austrian Labour Constitution Act (*Arbeitsverfassungsgesetz* – "ArbVG"); in particular, sections 96 and 96a ArbVG. For certain data processing activities (e.g., the implementation of control systems such as whistle-blowing mechanisms), the consent of the works council is mandatory (please see section 14 below). The relevant provisions of the ArbVG apply in addition to the "general" data protection laws (GDPR and DSG) with regard to employee data protection.

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

Other sector-specific legislation can, *inter alia*, 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 Austrian Banking Act (banking secrecy). Many other laws have been adapted due to the GDPR's entry into force, namely by two Material Data Protection Adaptation Acts (1. *Materien-Datenschutz-Anpassungsgesetz 2018*, BGBl. I Nr. 32/2018; and 2. *Materien-Datenschutz-Anpassungsgesetz 2018*, BGBl. I Nr. 37/2018).

1.4 What authority(ies) are responsible for data protection?

The *Datenschutzbehörde* ("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 required 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") means personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms, such as 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.
- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*

  "**Consent**" (of the data subject) means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

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) consent of the data subject for one or more specific purposes (for the requirements of an effective consent see definition above); (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 or social security 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**

  The procession of 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.
- **Proportionality**

  The requirement of proportionality (of data processing) is reflected in the GDPR in many provisions, e.g., in Art 5 para 1 *lit* c or Art 9 para 2 *lit* g GDPR. Furthermore, the principle of proportionality is explicitly mentioned in Article 84 GDPR with regard to penalties for violations of the GDPR, which need to be "effective, proportionate and dissuasive".
- **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.
- *Other key principles – please specify*

  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.

  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. In particular, the controller is obliged to implement

appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR.

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 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 live in Austria or the alleged infringement occurred in Austria.

- *Other key rights – please specify*

  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.

  Right not to be subject to automated individual decision-making

  Data subjects have the right not to be subject to a decision based solely on automated processing of data (including profiling), which produces legal effects or similarly significantly affects for the data subject. This right applies unless a decision: (i) is necessary for entering into, or performance of, a contract between the data subject and the controller; (ii) is authorised by Union or Member State law to which the controller is subject and which lays down suitable measures to safeguard the data subject's rights and legitimate interests; or (iii) is based on explicit consent. However, in these cases further requirements and exceptions apply.

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

The DSG provides, in its sections 7 and 8, 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 (section 7 DSG); and (b) in the context of processing address data of data subjects for the purposes of an important public interest regarding the notification or interview of those subjects (section 8 DSG).

In line with the principle of accountability, any controller and processor now has to keep a record detailing all processing activities. This record serves the purpose of proving compliance with the GDPR and has to be presented to the DSB at the request of the authority. This obligation does not apply to organisations that employ less than 250 persons unless the processing activities are likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences.

The DSB has stated in its official guideline to the GDPR (the latest version issued in January 2019) that all documentation to be provided to the DSB in the course of a(n) (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 of the private sector is only mandatory if their core activities include: (i) large-scale regular and systematic monitoring of individuals; or (ii) large-scale processing of sensitive personal data.

If 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 requirements.

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

Under circumstances where an appointment of a Data Protection Officer is mandatory, failure to comply with such obligation may result in the wide range of penalties available under the GDPR. In particular, the controller or processor is subject to an administrative fine of the higher of up to EUR 10 million 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 of his or her role as a Data Protection Officer?

The appointed Data Protection Officer should not be dismissed or penalised for performing his tasks (although no general dismissal protection exists) 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. In particular, the identity of any person who has contacted the Data Protection Officer has to be kept confidential. 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 group of undertakings may appoint a single data protection officer, provided that this person 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 may be a staff member of the controller or processor or fulfil the tasks on the basis of a service contract, should be appointed on the basis of professional qualities, and should have an expert knowledge of data protection law and practices. The Data Protection Officer should have the ability to perform the tasks outlined in question 7.6 below. 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 and the duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects, 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. For transfer of personal data to processors outside the EU, please see question 11.2 below.

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, which sets out the subject matter and duration as well as the nature and purpose of the processing, the type of personal data and categories of data subjects, and the obligations and rights of the controller. 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. Such prior consent is not 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 the sender's own similar products or services;
- the recipient clearly and distinctly has, at the time the electronic contact information was collected and furthermore on the occasion of each contact, 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 para 2 Austrian E Commerce Act).

For reasons of clarity, it is advisable to get prior consent from 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 must be obtained in advance. 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 (*Fernmeldebüro*); the data protection authority is not responsible for the enforcement of such violations. The *Fernmeldebüro* 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 Trade, Commerce and Industry Regulation Act (*Gewerbeordnung*) are entitled to collect (non-sensitive) data from publicly available sources (and to add classifications for specific marketing purposes) for the preparation and execution of marketing purposes for third parties. Furthermore, these undertakings are entitled to sell such lists to third parties and to act as an intermediary between the owners and users of marketing lists. The use of data contained in marketing lists of third parties without the consent of the data subjects is only possible for certain data (essentially name, address, date of birth, profession) and if the owner of the marketing lists declares in writing that the data subjects have been informed about the possibility to prohibit the transfer for marketing purposes of third parties, and have not pronounced such prohibition. The collection of any sensitive data requires the explicit consent of the data subject. Furthermore, 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 that is punishable by a fine of up to EUR 37,000.

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

In case the specific marketing communication infringes the GDPR, e.g. because data are used without compliance with Art 6 or Art 9 GDPR, the GDPR sanctions apply.

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 EU 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 the GDPR and before 25 May 2018 from Directive 95/46/EC). For the requirements of valid consent, compare the respective definition in section 2 above. 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 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

The WP29 published Working Document 02/2013 (WP 208), which provides 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 legally binding 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.

As outlined in question 10.1 above, section 96 para 3 TKG distinguishes between: cookies serving the sole purpose of carrying out the transmission of a communication via an electronic communications network or necessary to provide an "information society service" requested by the subscriber or user (which do not require the consent of the user); and any other 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 that 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 ("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. The EU Commission has issued decisions concerning an adequate level of protection for the following countries: Andorra; Argentina; Canada; Faroe Islands; Guernsey; Isle of Man; Israel; Jersey; New Zealand; Switzerland; and Uruguay.

11.2 Please describe the mechanisms businesses 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, one of which is via the consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses ("SCCs") or Binding Corporate Rules ("BCRs").

Businesses can adopt the SCCs drafted by the EU Commission – these are available for transfers among controllers, and transfers between a controller (as exporter) and a processor (as importer). International data transfers may also take place based on contracts agreed between the data exporter and data importer provided that they meet the protection standards 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 requirements 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's regular information and reporting channels, such as employee representatives, line management, quality-control personnel or internal auditors who are employed precisely to report such misconduct.

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, particularly in the light of the seriousness of the alleged offences reported.

Prior to the entry into force of the GDPR, the DSG issued several permits for whistle-blowing schemes subject to a set of conditions detailing the required procedural safeguards and the design of such systems (e.g., confidentiality with regard to the whistle-blower, access to accusation for the person concerned, deletion of data after the cessation of investigations). Although the pre-approval requirements do not apply any more, the authority will likely continue to apply these principles in an *ex post* control.

Notably, 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 an official authority or when the processing is authorised by EU or a Member State's law. In Austria, the now amended section 4 para 3 DSG provides for the processing of personal data relating to criminal offences (including suspicions about such offences), if such processing is necessary to safeguard

the legitimate interest of the controller or a third party and the interests of the data subject pursuant to the GDPR and the DSG are also safeguarded. Moreover, a specific statutory regulation for whistle-blowing hotlines exists in section 99g Austrian Banking Act (*Bankwesengesetz*).

Please note that the implementation of a whistle-blower scheme will likely require the consent of the works council pursuant to section 96 ArbVG and might require a DPIA.

12.2 Is anonymous reporting prohibited, 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 considering 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.

Similarly the DSB, in its formerly issued permits, stipulated that businesses implementing such schemes should not encourage anonymous reporting, but had to assure full confidentiality for anonymous whistle-blowers.

An individual who intends to report to a whistle-blowing system should be aware that he/she will not suffer reprisal 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 might need to be disclosed to the relevant people involved in any further investigation or subsequent judicial proceedings instigated because 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 experience gained in practice under the rules on CCTV that were contained in the DSG 2000.

In principle, CCTV is allowed if:

- it is required in the vital interests 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 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 happened in the past or there is a specific potential danger; or
- a private documentation interest in case the CCTV is directed neither to capture uninvolved persons in a way which allows their identification, nor to capture objects which would indirectly allow the identification of such persons.

In principle, CCTV needs to be specifically marked by a sign which identifies the respective controller (section 13 para 5 DSG). Moreover, any processing, except real-time surveillance, has to be logged (section 13 para 2 DSG).

The DSB has stated in its 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) recordings of persons in their strictly personal spheres of life (please see question 14.1 below); (ii) control of employees in the workplace (please see question 14.1 below); (iii) automation-supported comparison of personal data obtained by means of CCTV without consent or for personal profiling with other personal data; and (iv) 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 DSG provides that any recordings of personal data have 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 subparagraph 1 DSG provides that CCTV is prohibited at locations that are deemed to be part of the most personal areas 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 subparagraph 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 5 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. If 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 subparagraph 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 that 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 in place to meet the requirements of the GDPR. Depending on the security risk as well as the nature, scope and purpose of the processing activities, this may include: the encryption or pseudonymisation 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 organisational 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 obligation 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 natural persons. If the controller is in default with such obligation, the competent authority may require the controller to inform the data subject.

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

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).

The WP29 has issued guidelines on the data breach notification detailing requirements for data breach notifications (WP 250).

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 Power	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 Power	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 oneself 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's 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's 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.

Since the GDPR came into force, the DSB has not exercised the respective powers. However, the authority has issued bans under the old data protection regime in the past.

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

Since the GDPR came into force, the DSB has – as far as we are aware based on publicly available information – not exercised its powers against businesses established in other jurisdictions.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses 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.

The DSB began to apply the GDPR in its decisions and to enforce the rights of data subjects thereunder. With these initial rulings, the DSB in part clarified its approach to and interpretation of several provisions of the regulation.

The most noteworthy decisions so far concerned the right to erasure and the limits to the storage periods for personal data. With regard to the storing of personal data after the termination of a contractual relationship, the DSB emphasised that a statute of limitation by itself does not create a legal obligation of a controller that justifies the storage of personal data. The extent to which this ruling will be upheld, and will exclude data storage during statutory periods of limitation for asserting contractual claims such as liability, etc., remains to be seen. In this context, the DSB also stressed that the abstract possibility of future legal disputes does not justify the storage of data. Rather, a controller has to show which specific legal disputes might arise in the future and in what way such legal actions justify a need to store personal data. The authority acknowledged, for example, that the storage of personal data during the statutory period for the assertion of claims due to discrimination in an application procedure (plus reasonable extra time with regard to instigation of a legal action) is justified.

Another instructive decision concerned the consent requirement. Just recently, the DSB dismissed the complaint of a user of a media

website, who claimed a violation of his right to withdraw consent. The website in question could be used either with a fee-based subscription without any cookies, or free of charge but with the requirement of consent to the use of cookies. The DSB ruled that the user was offered a free choice between the two options, and that the consequences of the non-provision of consent (i.e. the subscription or the use of another medium of information) did not constitute a substantial disadvantage for the data subject.

Until March 2019, the DSG imposed fines for violations of the GDPR in only five cases; all these cases concerned prohibited video surveillance. In many other cases, the DSB has issued warnings.

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

Austria had earlier enacted an "implementation act" to the GDPR. With the subsequent Data Protection Deregulation Act 2018 (BGBl. I 24/2018), which attracted a lot of public and scientific attention, the Austrian legislature intended to ease the compliance requirements with regard to data protection for businesses. Section 11 DSG requires the data protection authority to respect the principle of proportionality in imposing fines pursuant to Article 83 GDPR. The authority primarily has to apply remedies such as issuing warnings instead of imposing fines, in case of first-time violations. In addition, section 4 para 6 DSG now limits the right to information of the data subject in cases where trade or business secrets of the controller are affected. This act raised the concern that the legislature might neutralise the strict approach of the GDPR.

Although another amendment of the DSG has been enacted (BGBl. I Nr. 14/2019), the intended limitation of the personal scope of application of the constitutional right to data protection, again, was not achieved. Therefore, the Austrian constitutional right to data protection continues to refer not only to natural persons, but also to legal entities.

Furthermore, the DSB has issued a Whitelist as well as a Blacklist in 2018, detailing the exemptions and, conversely, the unconditional obligations for conducting DPIAs in Austria.

As for the European legislation, it may be expected that the Commission will publish implementation guidelines and provisions where necessary. Among other important issues, adapted standard contractual clauses for the transfer of personal data to third countries could be decided upon in the near future. Moreover, the proposal for a new E-Privacy Directive is still pending in the legislative process (see Procedure File 2017/0003/COD).

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, life sciences, data protection as well as antitrust and competition law. Dr. Sonja Hebenstreit is a certified data protection officer (certified by Austrian Standards).

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 (Germany), 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.

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 life sciences, energy, information technology, financial institutions and insurance.

Current 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
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Financial Services Disputes
- 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