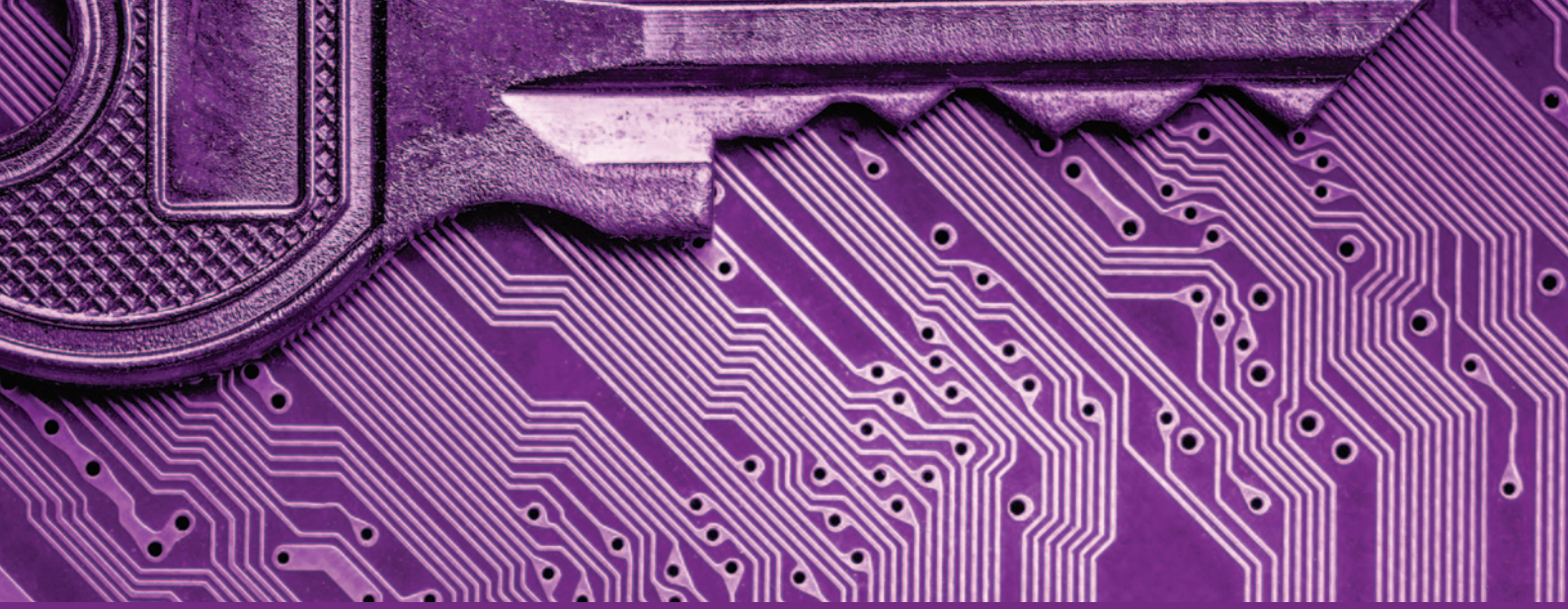

ICLG

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:

1	**The Rapid Evolution of Data Protection Laws** – Dr. Detlev Gabel & Tim Hickman, White & Case LLP	1
2	**The Application of Data Protection Laws in (Outer) Space** – Martin M. Zoltick & Jenny L. Colgate, Rothwell Figg	6
3	**Why Should Companies Invest in Binding Corporate Rules?** – Daniela Fábián Masoch, FABIAN PRIVACY LEGAL GmbH	12
4	**Initiatives to Boost Data Business in Japan** – Takashi Nakazaki, Anderson Mōri & Tomotsune	17

Country Question and Answer Chapters:

5	**Albania**	Deloitte Legal Shpk: Ened Topi & Emirjon Marku	22
6	**Australia**	Nyman Gibson Miralis: Dennis Miralis & Phillip Gibson	30
7	**Austria**	Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit	40
8	**Belgium**	Lydian: Bastiaan Bruyndonckx & Olivia Santantonio	51
9	**Brazil**	Vaz E Dias Advogados & Associados: José Carlos Vaz E Dias	62
10	**Canada**	Osler, Hoskin & Harcourt LLP: Adam Kardash & Patricia Kosseim	75
11	**Chile**	Rossi Asociados: Claudia Rossi	87
12	**China**	King & Wood Mallesons: Susan Ning & Han Wu	94
13	**Cyprus**	Koushos Korfiotis Papacharalambous LLC: Loizos Papacharalambous & Anastasios Kareklas	105
14	**Denmark**	Integra Law Firm: Sissel Kristensen & Heidi Højmark Helveg	115
15	**France**	Clyde & Co: Benjamin Potier & Jean-Michel Reversac	125
16	**Germany**	BEITEN BURKHARDT: Dr. Axel von Walter	136
17	**Ghana**	Addison Bright Sloane: Victoria Bright	146
18	**Hong Kong**	Ashurst Hong Kong: Joshua Cole & Hoi Tak Leung	154
19	**India**	Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam	168
20	**Indonesia**	Assegaf Hamzah & Partners: Zacky Zainal Husein & Muhammad Iqsan Sirie	183
21	**Ireland**	Matheson: Anne-Marie Bohan & Chris Bollard	191
22	**Isle of Man**	DQ Advocates Limited: Sinead O'Connor & Adam Killip	203
23	**Israel**	Herzog Fox & Neeman: Ohad Elkeslassy	212
24	**Italy**	Morri Rossetti e Associati – Studio Legale e Tributario: Carlo Impalà	221
25	**Japan**	Mori Hamada & Matsumoto: Hiromi Hayashi	230
26	**Korea**	Lee & Ko: Kwang Bae Park & Hwan Kyoung Ko	240
27	**Kosovo**	Deloitte Kosova Shpk: Ardian Rexha Deloitte Legal Shpk: Emirjon Marku	250
28	**Luxembourg**	thg IP/ICT: Raymond Bindels & Milan Dans	259
29	**Macau**	Rato, Ling, Lei & Cortés – Advogados: Pedro Cortés & José Filipe Salreta	269
30	**Malaysia**	Christopher & Lee Ong: Deepak Pillai & Yong Shih Han	279
31	**Malta**	GANADO Advocates: Dr. Paul Micallef Grimaud & Dr. Luke Hili	290
32	**Mexico**	OLIVARES: Abraham Diaz Arceo & Gustavo A. Alcocer	300
33	**Niger**	KADRI LEGAL: Oumarou Sanda Kadri	308
34	**Nigeria**	Infusion Lawyers: Senator Iyere Ihenyen & Rita Anwiri Chindah	314
35	**Norway**	Wikborg Rein Advokatfirma AS: Line Coll & Emily M. Weitzenboeck	324
36	**Pakistan**	S. U. Khan Associates Corporate & Legal Consultants: Saifullah Khan & Saeed Hasan Khan	336
37	**Portugal**	Cuatrecasas: Sónia Queiróz Vaz & Ana Costa Teixeira	343

Continued Overleaf

global legal group

Country Question and Answer Chapters:

38	**Senegal**	LPS L@w: Léon Patrice Sarr	354
39	**Singapore**	Drew & Napier LLC: Lim Chong Kin	362
40	**Spain**	Ecija Abogados: Carlos Pérez Sanz & Pia Lestrade Dahms	374
41	**Sweden**	Bird & Bird: Mattias Lindberg & Marcus Lorentzon	385
42	**Switzerland**	Pestalozzi Attorneys at Law: Lorenza Ferrari Hofer & Michèle Burnier	395
43	**Taiwan**	Lee and Li, Attorneys At Law: Ken-Ying Tseng & Sam Huang	405
44	**Turkey**	Çiğdemtekin Çakırca Arancı Law Firm: Tuna Çakırca & İpek Batum	414
45	**United Kingdom**	White & Case LLP: Tim Hickman & Matthias Goetz	423
46	**USA**	White & Case LLP: Steven Chabinsky & F. Paul Pittman	433

Germany

BEITEN BURKHARDT

Dr. Axel von Walter

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Since 25 May 2018, the principal data protection legislation in the EU has been Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**"). The GDPR repealed Directive 95/46/EC (the "**Data Protection Directive**") and has led to increased (though not total) harmonisation of data protection law across the EU Member States.

In addition to the GDPR, Germany has enacted the **Federal Data Protection Act** of 30 June 2017 (*Bundesdatenschutzgesetz* – "**BDSG**"), which specifies the principles and provisions of the GDPR for Germany.

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

The **Federal Telecommunications Act** (*Telekommunikationsgesetz* – "**TKG**") of 22 June 2004 (as amended by the Act of 29 November 2018) implements the requirements of Directive 2002/58/EC (as amended by Directive 2009/136/EC) (the "**ePrivacy Directive**"), which provides a specific set of privacy rules to harmonise the processing of personal data by the telecoms sector. In January 2017, the European Commission published a proposal for an ePrivacy regulation (the "**ePrivacy Regulation**") that would harmonise the applicable rules across the EU. In September 2018, the Council of the European Union published proposed revisions to the draft. The ePrivacy Regulation is still a draft at this stage and it is unclear when it will be finalised.

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

In Germany, statutory Federal laws as well as statutory State laws provide sector-specific provisions that directly or indirectly impact data protection. However, any German statutory law impacting data protection will be interpreted in accordance with the principles of the GDPR.

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

The Federal States (*Länder*) have jurisdiction for the enforcement of data protection laws. Accordingly, 16 State authorities are responsible for data protection in the private sector. The Federal Data Protection Commissioner is responsible for data protection in the telecommunications sector.

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**" 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 interests 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) must 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 relevant State authority, if the data subjects live in Germany or the alleged infringement occurred in Germany.

- **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?

No; in general, there is no legal obligation in Germany for a business to notify the data protection authority or any other governmental body in respect of its processing activities. Sector-specific obligations may apply in exceptional cases. For instance, processing of data relating to health insurance can require the notification of the competent supervisory authority.

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)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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)?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

6.10 Can the registration/notification be completed online?

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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

In general, there is no registration or notification required for data processing in Germany. Exceptional specific notification requirements are subject to the sector-specific provisions.

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.

According to Section 38 of the BDSG, in addition to Article 37 (1) (b) and (c) of Regulation (EU) 2016/679, the controller and processor shall designate a data protection officer if they constantly employ, as a rule, **at least 10 persons dealing with the automated processing of personal data**.

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

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.

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 their tasks and should report directly to the highest management level of the controller or processor.

The dismissal of an appointed Data Protection Officer is only permitted for good reason. After the activity as Data Protection Officer has ended, the Data Protection Officer may not be terminated for a year following the end of appointment, unless the employer has just cause to terminate without notice.

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 and is able to communicate in German language with German-based employees or competent authorities.

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 data protection impact assessments 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 (the "**WP29**") (now the European Data Protection Board (the "**EDPB**")) recommended in its 2017 guidance on Data Protection Officers 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 an agreement with the processor which sets out the subject matter for processing, the duration of processing, the nature and purpose of processing, the types 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.

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 of 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 relevant data protection authority; (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?).

Yes, prior consent is mandatory for the sending of electronic direct marketing (according to Article 13 of the ePrivacy Directive).

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.).

Telephone marketing requires prior consent according to local laws on unfair trade practices. Business-to-business telephone marketing consent may be assumed if specific circumstances may lead to the conclusion that the recipient may consent to such telephone activity in that specific case. Any objection against direct marketing activities of the recipient must be obeyed.

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

Yes, the requirements apply to any marketing activities targeting persons based in Germany regardless of the jurisdiction of the sender.

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

Yes, competent authorities follow complaints of consumers thoroughly and will enforce the rules on direct marketing very strictly.

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

The purchase of addresses or any other contact detail data for marketing purposes is not lawful under the administrative practice of enforcement of the GDPR in Germany.

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

The wide range of potential penalties and damages under the GDPR generally apply to marketing communications in breach of the GDPR. Additionally, such marketing activities will infringe the local laws on unfair trade practices, as well as the Act Against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb* – "**UWG**").

10 Cookies

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

Article 5 of the ePrivacy Directive has not yet been implemented in Germany, according to the Data Protection Authorities in Germany. Therefore, German authorities take the position that the GDPR has to be applied to cookies directly. Pursuant to the German Data Protection Authorities' legal opinion, following the principle of 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). For consent to be valid, it must be informed, specific, freely given and must constitute a real and unambiguous 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.

The EU Commission intends to pass a new ePrivacy Regulation that will replace the respective national legislation in the EU Member States. The ePrivacy Regulation is planned to come into force in 2019.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

Article 5 of the ePrivacy Directive has not yet been implemented in Germany, according to the Data Protection Authorities in Germany. The legal opinion of the German Data Protection Authorities 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?

No information on enforcement action related to cookies is publicly available yet. However, the Bavarian Data Protection Authority has conducted a test on cookie compliance and announced enforcement activities against non-compliance, for implementation in the near future.

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

The wide range of potential penalties and damages of the GDPR generally apply.

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), the business has implemented one of the required safeguards as specified by the GDPR, or one of the derogations specified in the GDPR applies to the relevant transfer. The EDPB Guidelines (2/2018) set out that a "layered approach" should be taken with respect to these transfer mechanisms. If the transfer is not to an Adequate Jurisdiction, the data exporter should first explore the possibility of implementing one of the safeguards provided for in the GDPR before relying on a derogation.

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, of which one is consent of the relevant data subject. Other common options are the use of Standard Contractual Clauses or 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 Binding Corporate Rules ("**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 USA 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, 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. In the Opinion it is recommended 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.

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 as regards the essential requirement that personal data should only be collected fairly. In the past, the German Data Protection Authorities took the position that anonymous whistle-blowing should not be permissible. In Opinion 1/2006, the WP29 considered that only identified reports should be advertised in order to satisfy the above-mentioned 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)?

A data protection impact assessment ("**DPIA**") must be undertaken with assistance from the Data Protection Officer when there is a systematic monitoring of a publicly accessible area on a large scale. If the DPIA suggests that the processing would result in a high risk to the rights and freedoms of individuals prior to any action being taken by the controller, the controller must consult the data protection authority.

During the course of a consultation, the controller must provide information on the responsibilities of the controller and/or processors involved, the purpose of the intended processing, a copy of the DPIA, the safeguards provided by the GDPR to protect the rights and freedoms of data subjects and where applicable, the contact details of the Data Protection Officer.

If the data protection authority is of the opinion that the CCTV monitoring would infringe the GDPR, it has to provide written advice to the controller within eight weeks of the request of a consultation and can use any of its wider investigative, advisory and corrective powers outlined in the GDPR.

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

According to Section 4 of the BDSG, monitoring publicly accessible areas with optical-electronic devices (video surveillance) shall be permitted only as far as it is necessary: (i) for public bodies to perform their tasks; (ii) to exercise the right to determine who shall be allowed or denied access; or (iii) to safeguard legitimate interests for specifically defined purposes and if there is nothing to indicate legitimate overriding interests of the data subjects.

For video surveillance of: (a) large publicly accessible facilities, such as sport facilities, places of gathering and entertainment, shopping centres and car parks; or (b) vehicles and large publicly accessible facilities of public rail, ship or bus transport, protecting the lives, health and freedom of persons present shall be regarded as a very important interest, according to Sec. 4 of the BDSG.

14 Employee Monitoring

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

According to Sec. 26 para. 1 of the BDSG, personal data of employees may be processed for the detection of criminal offences if actual evidence to be documented substantiates the suspicion that the data subject has committed a criminal offence in the employment relationship, the processing is necessary for the detection and the legitimate interest of the employee in the exclusion of the processing is not predominant; in particular, the nature and extent are not disproportionate with regard to the cause. This shall also apply to severe infringements of contractual duties from the employment relationship. Secret monitoring of employees' performance by technical means is not permitted. This includes video monitoring. However, monitoring for the purpose of ensuring data security or for any relevant safety purposes can be permissible on the legitimate interest basis. Information requirements under the GDPR have to be met at all times.

Employees' private communication in transit is subject to the secrecy of telecommunications according to Sec. 88 of TKG. Thus, monitoring of employees' private communication in transit is prohibited. Any infringement of telecommunications secrecy can constitute a criminal offence under the German Criminal Code.

Potential co-determination rights of existing works councils remain unaffected.

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

Generally, for monitoring that is not covered by statutory justification (see question 14.1 above), consent would be required.

However, according to Sec. 26 para 2 of the BDSG, where personal data of employees shall be processed on the basis of consent, the assessment of the voluntary nature of the consent must take into account, in particular, the employment dependence of the employee and the circumstances in which the consent was given. German authorities have been very reluctant in the past to consider consent in employment relationships as being given freely, due to the inherent

dependence of the employee on his/her employer. Nevertheless, voluntariness may exist, in particular, if a legal or economic advantage is obtained for the employee or if the employer and the employee pursue similar interests. Consent must be given in writing, unless another form is appropriate due to special circumstances. Further, the employer must inform the employee personally, in text form, of the purpose of the data processing and of his/her right of withdrawal pursuant to Article 7 para. 3 of the GDPR.

Notice is generally provided at the beginning of the employment relationship (e.g. as an information annex to the employment contract). It is also best practice to provide and update all general privacy-related information in an intranet resource. Particular information related to special data processing should be provided *ad hoc* in that particular processing context.

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

Any technical means to monitor behaviour or performance of employees are subject to works council approval before the beginning of such monitoring.

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 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 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 €20 million or 4% of worldwide turnover, provided that the data security breach is due to non-compliance of the controller with the requirements of the GDPR.

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 review 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
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).	N/A
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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Imposition of administrative fines for infringements of specified GDPR provisions	The GDPR provides for administrative fines which can be €20 million or up to 4% of the business' worldwide annual turnover of the preceding financial year.	The BDSG provides criminal law sanctions for: ■ Unlawful intentional transfer, on a commercial basis, of a large scale, of personal data not accessible to the public, to third parties. ■ Unlawful processing of personal data not accessible to the public whilst acting against payment or with the intention of enriching oneself or another or damaging another.
Non-compliance with a data protection authority	The GDPR provides for administrative fines which will be €20 million or up to 4% of the business' worldwide annual turnover of the preceding 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 to impose a temporary or definitive limitation including a ban on processing.

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

Germany's Data Protection Authorities (17 State authorities and 1 Federal authority) have followed independent and diverging approaches to exercising the available regulatory powers. It is said that authorities in northern Germany would be more likely to use sanctions for the enforcement of applicable data protection laws than authorities in the southern States of Germany. However, in general, German authorities follow a cooperative approach and, in case of data protection infringements (including data breaches), will reward the cooperation of businesses when applying enforcement measures.

Recent sanction cases include, for example:

- €50,000 against a fintech business for maintaining a customer blacklist without legal basis (State Authority of Berlin).
- €20,000 against a social network in a data breach case for not having encrypted users' passwords (State Authority of Baden-Wuerttemberg).
- €80,000 for unauthorised disclosure of health data by a hospital (State Authority of Baden-Wuerttemberg).

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

German data protection authorities will not refrain from exercising their powers against businesses established in other jurisdictions. Authorities would use the system of international enforcement treaties to enforce their powers. For instance, German authorities have exercised their powers against Facebook through its establishment in Ireland.

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?

Any data transfer in response to a foreign e-discovery must be lawful and in compliance with the provisions on international data transfer of the GDPR. Businesses will, in each case, assess both the legal basis for such data transfer and the adequacy of the level of data protection of the recipient. Businesses will, in most cases, refer foreign authorities to the system of international enforcement treaties. Strict retention policies, in compliance with the principle of storage limitation, will help businesses to keep to a minimum the amount of data they hold which is subject to e-discovery or disclosure.

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

The Article 29 Data Protection Working Party has issued the *Working Document 1/2009 on pre-trial discovery for cross border civil litigation* (WP158, adopted 11 February 2009) for further guidance. Although the Article 29 Data Protection Working Party ceased to exist on 25 May 2018 and the European Data Protection Board did not formally adopt all documents of the Article 29 Data Protection Working Party, the Working Document 1/2009 will still have persuasive effect and remains an important resource for guidance.

18 Trends and Developments

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

After a phase of consultation and support for businesses in the implementation of the requirements of the GDPR, German authorities began to make use of their enforcement powers in the second half of the year. The focus of enforcement activities was on the handling of data subject complaints and the enforcement of data subject rights, including the right to be forgotten. Reported administrative fines mostly dealt with unlawful data access.

For recent sanction cases, please see question 16.3 above.

The State authorities are currently working on uniform guidelines for the imposition of fines in Germany to ensure a coherent enforcement of the GDPR in Germany.

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

German Data Protection Authorities take the position that the ePrivacy Directive has not yet been properly implemented in German law. Thus, the requirements of the GDPR apply directly to the use of cookies, and any tracking-related cookies would require consent. In February 2019 the Bavarian authority conducted an audit of the websites of 40 companies in Bavaria regarding cybersecurity and tracking technologies, and found that no website complied with the applicable requirements of the GDPR.

In the light of the recent case law of the European Court of Justice (e.g. judgment of 5 June 2018, C-210/16), German State authorities are debating the concept of joint controllership; in particular, in the context of the use of Facebook fan pages. In April 2019 German State authorities took the position that Facebook fan pages cannot be used in compliance with the GDPR by German companies.

The Bavarian authority announced a review of the ability to delete data within enterprise resource planning ("ERP") software systems for 2019. Companies are advised to implement appropriate deletion concepts in their organisations.

Data subject rights will remain in the focus of the State authorities.

Dr. Axel von Walter
BEITEN BURKHARDT
Ganghoferstrasse 33
Munich
Germany

Tel: +49 89 35065 1321
Email: axel.walter@bblaw.com
URL: www.beiten-burkhardt.com

Dr. Axel von Walter, CIPP/E, CIPM is a Partner at BEITEN BURKHARDT's Munich office and a member of the management board of the firm. He advises his clients on all areas of data protection, cyber security and information law, as well as competition law. In addition to operational advice, Dr. von Walter has extensive experience in litigation, particularly injunctive relief.

After studying law at the University of Munich, he was admitted to the German Bar in 2004. He has been Partner at BEITEN BURKHARDT since 2011. Before joining BEITEN BURKHARDT, he had been working for other international law firms in the field of IP/IT, media and data protection law, among others, in London. His doctoral thesis was awarded the Faculty Award of the faculty of law of the University of Munich.

Dr. von Walter is a lecturer in media and information law at the faculty of law at the University of Munich, and he is CIPP/E and CIPM-certified under the IAPP certification scheme for privacy professionals. He is frequently listed in the leading law firm rankings as a recommended lawyer (including *The Legal 500* and *JUVE*).

BEITEN BURKHARDT

BEITEN BURKHARDT's privacy and cyber security team helps companies manage privacy and cyber security-related compliance requirements, and mitigate risks at every step of the data life cycle.

We understand data-driven business models and how data flows generate revenue for our clients. Our attorneys provide strategic advice on all legal aspects of data-driven businesses including data ownership, data protection compliance, cross-border data flows and data protection-related litigation. We assist with the acquisition, sale and financing of data-driven businesses.

Our privacy and cyber security team also advises businesses on all aspects of cyber security regulatory compliance, including critical infrastructure security, cyber security audits and cyber security breaches.

In cases of cyber security breaches, including data breaches, we are able to assist our clients 24/7/365 with their investigations, the identification of appropriate next steps, dealing with regulatory and customer notifications, and liaising with law enforcement and data protection authorities.

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