This article appeared in the 2014 edition of The International Comparative Legal Guide to: Data Protection; published by Global Legal Group Ltd, London. www.iclg.co.uk

ICLG

The International Comparative Legal Guide to:

Data Protection 2014

1st Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

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

GLG
Global Legal Group

GLG
Global Legal Group

Contributing Editor
Bridget Treacy,
Hunton & Williams

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

Sales Support Manager
Toni Wyatt

Sub Editors
Nicholas Catlin
Amy Hirst

Editors
Beatriz Arroyo
Gemma Bridge

Senior Editor
Suzie Kidd

Global Head of Sales
Simon Lemos

Group Consulting Editor
Alan Falach

Group Publisher
Richard Firth

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

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
May 2014

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

Strategic Partners

General Chapter:

Country Question and Answer Chapters:

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

EDITORIAL

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

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

It is divided into two main sections:

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

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

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

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

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

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

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

Germany

Dr. Jörg Hladjk

Hunton & Williams

Johannes Jördens

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is the Federal Data Protection Act (*Bundesdatenschutzgesetz*) (the "FDPA"), which was last amended in 2009 and implements into German law the requirements of the EU Data Protection Directive (95/46/EC) (the "Data Protection Directive"). Where no other law is referred to, references in the following responses to "sections" are references to sections of the FDPA.

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

The sixteen German federal states have state-level data protection laws. These laws only apply to the public sector in the relevant state.

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

The Telecommunications Act (*Telekommunikationsgesetz*) contains sector-specific data protection provisions that apply to telecommunications services providers such as internet access providers. The Telemedia Act (*Telemediengesetz*) also contains sector-specific data protection provisions that apply to telemedia service providers such as website providers.

Specific rules for online marketing (email, SMS, MMS) are set out in the Unfair Competition Act (*Gesetz gegen den unlauteren Wettbewerb*).

Canon law and postal data protection law also contain separate data protection provisions amongst other sector specific laws for the public sector.

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

There are seventeen state data protection authorities which oversee and enforce private and public sector data protection compliance of entities established in their state. The federal data protection commissioner (*Bundesdatenschutzbeauftragter*) oversees and enforces data protection compliance within the federal public sector (e.g., federal ministries) as well as certain parts of the postal services and telecommunications services providers' activities.

2 Definitions

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

- **"Personal Data"**

  "Personal data" means any information concerning the personal or material circumstances of an identified or identifiable natural person.

- **"Sensitive Personal Data"**

  "Special categories of personal data" means information on racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life.

- **"Processing"**

  "Processing" means the recording, alteration, transfer, blocking and erasure of personal data. Specifically, irrespective of the procedures applied:

  1. "recording" means the entry, recording or preservation of personal data on a storage medium so that they can be further processed or used;
  2. "alteration" means the modification of the substance of recorded personal data;
  3. "transfer" means the disclosure of personal data recorded or obtained by data processing to a third party either a) through transfer of the data to a third party, or b) by the third party inspecting or retrieving data available for inspection or retrieval;
  4. "blocking" means the identification of recorded personal data so as to restrict their further processing or use; and
  5. "erasure" means the deletion of recorded personal data.

- **"Data Controller"**

  "Controller" means any person or body which collects, processes or uses personal data on his, her or its own behalf, or which commissions others to do the same.

- **"Data Processor"**

  The FDPA uses the term "Data Processor" without explicitly defining it. The closest to a formal definition is Section 11 (1) Sentence 1 which reads "If other bodies collect, process or use personal data on behalf of the controller, the controller shall be responsible for compliance with the provisions of this Act and other data protection provisions".

- **"Data Owner"**

  "Data Owner" is not defined.

- **"Data Subject"**

  "Data Subject" means an identified or identifiable natural person.

- **"Pseudonymous Data"**

  "Pseudonymous Data" is not defined. However, "pseudonymizing" means replacing the data subject's name and other identifying features with another identifier in order to make it impossible or extremely difficult to identify the data subject.

- **"Direct Personal Data"**

  "Direct Personal Data" is not defined.

- **"Indirect Personal Data"**

  "Indirect Personal Data" is not defined.

- **Other key definitions**

  "Anonymizing" means the alteration of personal data so that information concerning personal or material circumstances cannot be attributed to an identified or identifiable natural person or that such attribution would require a disproportionate amount of time, expense and effort.

3 Key Principles

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

- **Transparency**

  There are two transparency requirements enshrined in the FDPA. The first is set out in section 4 (2). This section states that personal data must be collected directly from the data subject and they may only be collected without the data subject's involvement if it is legally required or if, broadly, the processing purpose necessitates an indirect collection and this indirect collection passes the balancing of interests test.

  The second transparency requirement is that the data subject be informed about the collection and processing of personal data relating to him or her.

  Where personal data are collected from the data subject, section 4 (3) requires that, if the data subject is not already aware of it, the data controller inform him/her as to: (i) the identity of the controller; (ii) the purposes of collection, processing or use; and (iii) the categories of recipients, if the data subject has no expectation that his/her data will be transferred to such recipients in the particular case.

  Where personal data are stored without the data subject's knowledge, section 33 (1) requires that the data subject be informed of the type of data, the purpose of the collection, processing or use, the identity of the data controller and the categories of recipients, if the data subject has no expectation that his/her data will be transferred to such recipients in the particular case.

- **Lawful basis for processing**

  Section 4 (1) states that the collection, processing and use of personal data is only lawful if the FDPA or another law permits or requires it, or if the data subject has consented.

  The main legal bases set out in the FDPA are: section 28 (data collection and storage for own commercial purposes), section 32 (data collection, processing and use for employment purposes), section 4 (1) and 4a (consent) and section 29 (commercial data collection and storage for transfer purposes).

- **Purpose limitation**

  Where personal data is processed on the basis of section 28 (data collection and storage for own commercial purposes), the purpose of the data processing and use must be determined at the time of collection. Section 28 (2) permits a change of purpose if it passes the balancing of interests test, the personal data are publicly available, it is required to safeguard a third party's lawful interests, it is required to guard against dangers to the state or public, or it is for research purposes which clearly outweigh the data subject's legitimate interests.

- **Data minimisation**

  Section 3a sets out the principles of data minimisation and data economy. The section states that as little personal data as possible should be collected, processed and used, and data processing systems should be chosen and organised accordingly. Further, personal data should be anonymised or pseudonymised if and when the purpose for which they are processed allows it and provided that the effort involved here is not disproportionate.

- **Proportionality**

  The proportionality principle is reflected throughout the FDPA. It is used both where particular operations *vis-à-vis* personal data are concerned (e.g., when personal data should be anonymised (section 3a)) as well as in the form of the balancing of interests test to determine whether a particular legal basis applies (e.g., section 28).

- **Retention**

  Section 35 (2) Nr. 3 states that personal data that are processed for the data controller's own purposes must be deleted when they are no longer required for the purpose for which they are stored. If personal data are stored for commercial transfer purposes, their continued storage must be evaluated every 3 or 4 years to determine whether they are still needed.

4 Individual Rights

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

- **Access to data**

  The data subject's right of access is mainly set out in section 34 and concerns access to information about: (1) recorded data relating to them, including information relating to the source of the data; (2) the recipients or categories of recipients to which the data are transferred; and (3) the purpose of recording the data.

  Data subjects have to be specific about the type of personal data about which information is to be given. Where the personal data are stored for commercial transfer purposes, the data subject must be provided with information about the personal data's source and recipients, even where such details are not recorded. The latter information can be withheld, though, if the interest in safeguarding trade secrets outweighs the data subject's interest in being provided with the information.

  More detailed provisions apply where scoring (e.g., credit scores calculated by credit reference agencies) and commercial data transfers are concerned.

  Information should be provided in writing and free of charge, unless any of the exemptions set out in section 34 apply.

- **Correction and deletion**

  The data subject's rights of correction, deletion and blocking are codified in section 35. Personal data must be corrected if they are inaccurate. They can be deleted at any time unless certain exemptions apply and they must be deleted if: (a) their storage would be unlawful; (b) they concern racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health or sex life, or

criminal or administrative offences the accuracy of which the data controller cannot prove; (c) they are processed for own purposes and they are no longer required for the purpose for which they are stored; or (d) they are processed for commercial transfer purposes and their retention is no longer required.

In certain circumstances, personal data must be blocked instead of deleted.

- **Objection to processing**

  The data subject's general right to object to the processing of his/her personal data is set out in section 35 (5). This section states that personal data must not be collected, processed or used if the data subject has objected and if an evaluation of the data subject's specific personal circumstances shows that his/her legitimate interests outweigh the data controller's legitimate interests in collecting, processing or using his/her personal data.

  In addition to this general right to object, the FDPA contains more specific rights to object to certain types of processing.

- **Objection to marketing**

  Section 28 (4) of the FDPA states that if the data subject has objected to the processing of his/her personal data for marketing purposes or for the purposes of market or opinion research, then the personal data must not be processed or used for these purposes.

  Section 7 (1) of the Unfair Competition Act states that sending advertisements to a recipient who clearly does not wish to receive advertisements is unlawful.

  In an online context, section 15 (3) of the Telemedia Act states that telemedia service providers may only use pseudonymised usage profiles for marketing purposes if the user has not objected. The user must be specifically informed about his/her right to object.

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

  The FDPA does not formalise a complaints procedure. However, it is common for data subjects to contact the relevant data protection authority and for the data protection authority to then investigate the complaint.

5 Registration Formalities and Prior Approval

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

There is a general requirement in section 4 to notify the relevant data protection authority of the automated processing of personal data. However, this general notification requirement does not apply if the data controller has appointed a data protection officer. It also does not apply if only up to nine staff process personal data for the data controller's own purposes on the basis of consent or for the purpose of the creation, performance of termination of a contractual or quasi-contractual relationship with the data subject.

Nonetheless, a notification is always required if personal data are processed: (a) for commercial transfer purposes (e.g. for address selling businesses); (b) for anonymised commercial transfer purposes; or (c) for market and opinion research purposes.

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

Each automated processing operation must be notified.

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

All entities to whom German data protection law applies and who cannot avail themselves of either of the exceptions to the general duty to notify must file notifications with the relevant data protection authority. This may include foreign legal entities as well as their German representative or branch offices.

Whether German data protection law applies is determined under section 1.

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

The content of the notification is prescribed in section 4e as:

- name or company name of the data controller;
- owners, management boards, managing directors or other company leaders appointed by law or by the company's regulations, and the persons in charge of data processing;
- the data controller's address;
- the purposes of the data collection, processing or use;
- a description of categories of data subjects and the data or categories of data relating to them;
- the recipients or categories of recipients to whom the data can be disclosed;
- standard retention periods for the data;
- intended transfers of the data to third countries; and
- a general description allowing a preliminary assessment of whether the security measures implemented in accordance with section 9 are appropriate.

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

The sanction is €50,000 (section 43(3) and (1) Nr. 1).

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

Generally, there is no notification fee.

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

The notifications must be updated before the data processing is changed as well as before its termination (section 4e).

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

Section 4d (5) requires that if automated processing operations are particularly risky for the rights and freedoms of the data subjects, then they must be analysed before any processing starts. This analysis or "prior checking" will be required especially where sensitive personal data are processed or where the processing is intended to evaluate the data subject's personality, performance or behaviour. It is, however, not required where the processing is required by law, required for the creation, performance of

termination of a contractual or quasi-contractual relationship with the data subject or where the data subject has consented.

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

The data controller's data protection officer is responsible for carrying out the prior checking. He/she must carry out the prior checking after having received an overview of the relevant processing operation from the data controller and can involve the relevant data protection authority as required (section 4d (6)).

6 Appointment of a Data Protection Officer

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

There is a general requirement in section 4f (1) to appoint a data protection officer. However, this general notification requirement does not apply if only up to nine staff process personal data regularly.

Nonetheless, a data protection officer will always have to be appointed if the entity in question uses automated means to processes personal data that are subject to prior checking or for the purposes of commercial data transfer, anonymised commercial transfer or market or opinion research.

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

The relevant entity may be fined up to €50,000 and the relevant data protection authority may order it to appoint a data protection officer.

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

The majority of businesses in Germany will already have to appoint a data protection officer by law so voluntary appointments of data protection officers are rare.

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

The data protection officer must possess the necessary expertise and reliability in order to fulfil his/her responsibilities (section 4f (2)). The German data protection authorities issued more detailed guidance (dated 4/5 November 2010) on what level of qualification and expertise is typically expected. According to this guidance, all data protection officers should have:

- basic knowledge of the personality rights granted by the German Constitution to the customers and employees of the data controller; and
- comprehensive knowledge of the FDPA, including technical (e.g., data security measures) and organisational (e.g., concepts of availability, authenticity and integrity of data) rules.

Additional areas of expertise will be required depending on the data controller's size, industry sector, IT infrastructure and sensitivity of the personal data processed.

Furthermore, the data protection officer must be independent within the company and report directly to German management.

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

The DPO must work towards compliance with the FDPA and other data protection provisions (e.g., data protection provisions in the Telemedia Act). In particular, the FDPA requires the DPO to undertake the following tasks:

- Monitor how data processing software is used to process personal data and verify that the processing is compliant with relevant data protection provisions.
- Take appropriate measures to educate and train individuals processing personal data about the provisions of the FDPA and other relevant data protection provisions.
- If the company is not required to notify its processing to the DPA, the DPO must provide the public data processing inventory to those who request it. The company must provide the DPO with the data inventory.
- Where a prior checking is required, the DPO is responsible for carrying it out.

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

No, this is not the case.

7 Marketing and Cookies

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

The Unfair Competition Act generally requires the recipient's consent if marketing messages are sent to him/her by phone, SMS, fax or email. There are exceptions, though. As regards email, for example, section 7(3) of the Unfair Competition Act allows marketing emails to be sent without the recipient's consent where:

- the company obtained the recipient's email address from the recipient in connection with the sale of a good or a service;
- the company uses the email address to advertise directly for similar and own goods or services;
- the recipient has not objected to such use; and
- at the time the email address is collected as well as each time it is used, the recipient is informed clearly and unambiguously that he/she can object to such use at any time without incurring transmission costs which exceed the basic transmission tariffs.

For certain types of marketing activities (e.g., marketing list data), more detailed regulations apply (e.g., section 28 (3)).

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

Yes. Enforcement action as well as litigation concerning breaches of marketing restrictions are frequent in Germany.

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

Breaches of the Unfair Competition Act's marketing restrictions can result in fines of up to €300,000 (section 20 (2) of the Unfair Competition Act).

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

There are currently conflicting interpretations of the applicable law. The German government's position is that only those cookies that are strictly necessary for the user to receive telemedia services (e.g., to view a website) can be used without the user's prior opt-in consent. The German government's position is outlined in a communication to the European Commission (COCOM11-20) dated 04 October 2011 and relies on section 15 (1) of the Telemedia Act.

The German data protection authorities, however, state that an opt-out approach is generally appropriate for cookies. Their argument is based on §15 (3) of the Telemedia Act and set out in a resolution dated 24/25 November 2010.

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

Please refer to the answer above. The position is currently not settled in Germany.

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

The Bavarian data protection authority has analysed various web analytics tools in detail and made recommendations on how such tools can be used in a compliant manner. Cookies and opt-out methods played a central role in these analyses.

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

Breaches of the relevant provisions of the FDPA could result in fines of up to €300,000. Breaches of the relevant provisions of the Telemedia Act could result in fines of up to €50,000.

8 Restrictions on International Data Transfers

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

International transfers of personal data subject to German law must pass a two-stage test. The first stage is whether there is a legal basis for transferring the personal data to a third party since there is no privilege for sharing data within a group of companies. The second stage is whether the personal data will be afforded an adequate level of protection in the country to which they are transferred (section 4b) or whether an exception applies (section 4c).

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

Companies typically use EU Standard Contractual Clauses to transfer personal data to countries outside the EEA. For international transfers within a corporate group, Binding Corporate Rules are becoming increasingly common.

Transfers to Companies that are certified under the Safe Harbor Framework Agreement remain common, too. However, the adequacy of the Safe Harbor Framework has been repeatedly questioned by the German data protection authorities.

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

No. However, the German data protection authorities have the power to authorise individual transfers on an *ad-hoc* basis, where other international data transfer mechanisms do not apply (section 4c (2)). At the time of writing, though, the German data protection authorities have suspended granting such *ad-hoc* authorisations (see the German data protection authorities' press release dated 24 July 2013).

9 Whistle-blower Hotlines

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

The German data protection authorities have issued formal guidance on the scope of whistleblowing hotlines (see the data protection authorities' April 2007 working paper). According to the guidance, the following matters are within the permitted scope:

- Any conduct which constitutes a crime and affects the interests of the business. This includes, for example, fraud and fraudulent accounting, corruption, financial crimes, and illegal insider dealing.
- Any conduct in breach of human rights. This includes, for example, the use of child labour.
- Any conduct in breach of environmental protection rules.

It may also include substantial, serious breaches of lawful and clear company policies but this has to be evaluated on a case-by-case basis.

The data protection authorities also recommend that companies review whether it is possible to restrict the scope of persons who may submit reports. They recognise, however, that this requires a case-by-case evaluation.

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

According to the German data protection authorities' guidance, anonymous reporting is strongly discouraged. It is recommended that whistleblowers are informed that their identify will be treated confidentially and that whistleblowers are not disadvantaged as a result of filing a report.

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

Where a company has appointed a data protection officer, there is

no requirement to make a notification to the relevant data protection authority. However, it is likely that the data protection officer has to conduct a formal prior checking before the whistleblowing system is deployed. The length of this prior checking depends on the complexity of the whistleblowing system and can range from days to months. The data protection officer will also have to update the processing inventories.

10 CCTV and Employee Monitoring

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

Where a company has appointed a data protection officer, there is no requirement to make a notification to the relevant data protection authority. However, it is likely that the data protection officer has to conduct a formal prior checking before the CCTV system is deployed. The data protection officer will also have to update the processing inventories.

Section 6b regulates in detail how publicly accessible premises may be monitored via CCTV and the data protection authorities have issued guidelines on CCTV implementation.

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

Employee monitoring is only permitted in very limited circumstances since the relevant legal basis (section 32) is a specific provision for employee data processing. For example, data controllers may process personal data of employees if it is necessary to discover crimes but only if: (a) there are documented factual indications which support the suspicion that the employee has committed a crime in the course of the employment relationship; (b) the processing of personal data is necessary to discover the crime; and (c) the protected privacy interests of the employee do not take precedence.

Permanent monitoring of employees via CCTV is usually not permitted and companies have been fined for doing so. Sporadic monitoring for quality and training purposes (e.g., listening in on customer calls) may be lawful provided it is not excessive and the relevant legal requirements (e.g., notice) are met.

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

In an employment context, data protection authorities consider that consent is not a valid legal basis for the processing of personal data since employees are rarely free to give or withhold consent demanded by the employer. Therefore, the employer needs to ensure that any monitoring of employees that involves the processing of personal data is covered by section 32.

In addition to the legal basis, the employer must provide advance and sufficiently detailed notice of any employee monitoring. Where the employer has a works council, a works council agreement will usually be required to legitimise the employee monitoring. Employees must then be made aware of these works council agreements which is usually done by email or another type of prominent notice.

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

Section 87 Nos. 1 and 6 of the Works Constitution Act (*Betriebsverfassungsgesetz*) requires that the works council must be informed about and agree to all measures that concern how the employees' behaviour is regulated and whenever technical means to monitor the employees' behaviour and performance are to be introduced. This process usually takes several months.

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

Where a company has appointed a data protection officer, there is no requirement to make a notification to the relevant data protection authority. However, it is likely that the data protection officer has to conduct a formal prior check before the employee monitoring measures are deployed. The data protection officer will also have to update the processing inventories.

11 Processing Data in the Cloud

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

Yes, personal data may be processed in the cloud provided all legal requirements are met. In their detailed guidance (dated 26 September 2011), the German data protection authorities identified five areas where specific due diligence by the data controller is required:

- The risk of re-identification of anonymised data.
- The data protection obligations of all parties involved in providing the cloud service (including sub-processors).
- The data controller's continued ability to comply if a data subject exercises his/her rights of access, correction, deletion and blocking.
- The lawfulness of any international transfers of personal data in the context of the cloud services.
- The presence and verification of appropriate technical and organisational security measures, particularly concerning deletion, data separation, transparency, data integrity, back-ups and audit functions.

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

The FDPA's requirements for data processing agreements must be met. These are mainly set out in section 11 and include contractual provisions concerning:

- the subject and duration of the data processing;
- the extent, type and purpose of the intended collection, processing or use of data, the type of data and category of data subjects;
- the technical and organisational security measures to be implemented pursuant to section 9;
- the rectification, erasure and blocking of data;

- the processor's obligations under section 11 (4), in particular as regards monitoring the data processing;
- any right to appoint sub-processors;
- the data controller's rights to monitor and the data processor's corresponding obligations to accept such monitoring and cooperate with the data controller;
- notification obligations where the data processor or its employees breach applicable data protection law or the contract;
- the extent of the data controller's authority to issue instructions to the data processor; and
- the return of data storage media and the erasure of data recorded by the data processor at the end of the data processing.

12 Big Data and Analytics

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

Yes, provided the processing involved in the analysis of the personal data is covered by a legal basis and the remaining provisions of the FDPA (e.g., regarding notice) are complied with.

In practice, the Baden-Wurttemberg data protection authority states in its 2013 report that the principles of data minimisation and data economy should be reflected in the design of big data platforms. Where anonymisation and pseudonymisation are used, it should be ensured that the risk of re-identification is properly taken into account.

13 Data Security and Data Breach

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

Section 9 and its annex set out the legally required data security measures that must be applied when personal data are processed, namely:

1. measures to control who has physical access to the personal data;
2. measures to control who has virtual access to the personal data;
3. measures to enforce limits on user access rights;
4. measures to control to whom personal data are disclosed;
5. measures to monitor and log any input, modification or deletion of personal data;
6. measures to control subcontractors;
7. measures to ensure availability of the personal data; and
8. measures to ensure that personal data collected for different purposes are used separately and not mixed.

The FDPA recognises that state of the art encryption is particularly suitable as a type of security measure listed under Nos. 2 to 4 above.

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

Yes, section 42a requires that in the circumstances described below, the competent data protection authority as well as the affected individuals must be informed without undue delay.

The circumstances in which section 42a applies are that there is an unlawful transfer or other disclosure to third parties of the following types of personal data and there is a danger of serious adverse effects against the rights or protected interests of the affected individuals.

The types of personal data which are within the scope of this section are:

- sensitive data as defined in the FDPA;
- personal data that are subject to professional or official confidentiality obligations;
- data concerning criminal acts or administrative offences;
- bank or credit card account details;
- customer data or traffic data as defined in the Telecommunications Act (e.g., subscriber personal data and traffic data); and
- customer data or usage data as defined in the Telemedia Act (e.g., registration or usage data that may identify an individual user).

The data protection authorities have issued detailed guidance on section 42a.

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

Yes, where section 42a applies, the data controller must notify the affected individuals as soon as appropriate measures to secure the relevant data have been implemented and any criminal prosecution is no longer endangered.

Each affected individual must be provided with information about the kind of data breach and about ways of mitigating any adverse effects on their interests.

14 Enforcement and Sanctions

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

Investigatory Power	Civil/administrative Sanction	Criminal Sanction
Conduct inquiries (section 38 (3))		
Conduct on-site audits (section 38 (4))		

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Impose compliance orders, including prohibiting individual processing operations (section 38 (5))	Impose fines until order is complied with	
Require the appointment of a different data protection officer (section 38 (5))		
Inform data subjects about breaches of data protection law (section 38 (1))		
Inform responsible criminal prosecutor about breaches of data protection law (section 38 (1))		
Inform other competent supervisory authorities about breaches of data protection law (section 38 (1))		
	Impose administrative fines of up to €50,000 under section 43(1) (if the state data protection law has transferred this power to the state data protection authority)	
	Impose administrative fines of up to €300,000 under section 43(2) (if the state data protection law has transferred this power to the state data protection authority)	
		Apply to the competent criminal prosecutor under section 44 (2) which can trigger sanctions of up to two years' imprisonment, as well as a fine

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

German data protection authorities exercise their enforcement powers reasonably frequently. Most common are audits (whether by way of questionnaire or on-site inspection) as well as specific compliance orders. Where serious breaches occurred or orders are not complied with, German data protection authorities impose fines.

Notable cases are a €1.1 million fine imposed on Deutsche Bahn for multiple breaches of the FDPA as well as a €1.5 million fine imposed on the Lidl group for using private detectives and secret cameras in their German shops.

Recent cases concerned Hamburg DPA's €54,000 fine of Europcar for using GPS trackers in certain rental cars.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

In our experience, German companies tend to refer foreign public authorities to the relevant mutual legal assistance treaties so that disclosures of personal data are done in a manner compliant with German data protection law. Where e-discovery requests are concerned, German companies tend to pseudonymise or anonymise the relevant materials first, before they are transferred.

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

Where direct disclosure requests/orders by foreign public authorities are concerned, the German data protection authorities have stated that the relevant German authorities should be involved immediately so that the disclosure can be done in accordance with relevant mutual legal assistance treaties (see the Berlin data protection authority's statement dated 14 November 2008 as well as the German Federal Ministry of Justice's letter to the Berlin data protection authority dated 31 January 2007).

As regards foreign e-discovery requests/orders, the German data protection authorities' position is that in light of the the Article 29 Working Party's paper on this topic (WP 158) as well as the Hague Convention, there must not be a transfer of personal data abroad before proceedings have been issued (i.e., pre-trial). Once the proceedings are underway, though, personal data can be transferred in pseudonymised form and data such as individual names may be de-pseudonymised as required on a case by case basis (see section 11.3 of the the Berlin data protection authority's 2009 report).

Dr. Jörg Hladjk

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 5828
Fax: +32 2 643 5822
Email: jhladjk@hunton.com
URL: www.hunton.com

Jörg is German qualified and advises multinational clients of all industry sectors on a broad range of EU data protection and cybersecurity matters, including German state and federal data protection law compliance. He has particular experience in developing strategies for international data transfers and regularly advises clients on issues such as data breach notification, cloud computing, smart grids, big data and e-discovery. He also has significant experience in contentious data protection matters and regularly represents clients before the German state and federal data protection authorities. Jörg was recognised as one of the world's leading practitioners by The International Who's Who for Information Technology Lawyers 2013 and has written extensively on data protection and IT security compliance topics.

Johannes Jördens

Hunton & Williams
Park Atrium
Rue des Colonies 11
1000 Brussels
Belgium

Tel: +32 2 643 5849
Fax: +32 2 643 5822
Email: jjordens@hunton.com
URL: www.hunton.com

Johannes advises multinational clients on all aspects of data protection and information technology law. He is dual-qualified in German and English law and has spent time on secondment to several businesses in the financial, utilities and TMT sectors. His data protection work includes advising on security incidents and complex data flows, as well as the implementation of comprehensive compliance regimes. He also advises on wider technology, software and content licensing matters, e-commerce agreements and on and offshore outsourcings.

HUNTON& WILLIAMS

Hunton & Williams' Global Privacy and Cybersecurity practice is a leader in its field. It has been ranked by Computerworld magazine for four consecutive years as the top law firm globally for privacy and data security. Chambers and Partners ranks Hunton & Williams the top privacy and data security practice in its Chambers & Partners UK, Chambers Global and Chambers USA guides.

The team of more than 25 privacy professionals, spanning three continents and five offices, is led by Lisa Sotto, who was named among The National Law Journal's "100 Most Influential Lawyers". With lawyers qualified in six jurisdictions, the team includes internationally-recognised partners Bridget Treacy and Wim Nauwelaerts, former FBI cybersecurity counsel Paul Tiao, and former UK Information Commissioner Richard Thomas.

In addition, the firm's Centre for Information Policy Leadership, led by Bojana Bellamy, collaborates with industry leaders, consumer organisations and government agencies to develop innovative and pragmatic approaches to privacy and information security.

Other titles in the ICLG series include:

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

GLG
Global Legal Group

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

www.iclg.co.uk