ICLG

The International Comparative Legal Guide to:

Data Protection 2018

5th Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

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

glg
global legal group

global legal group

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

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Sub Editor
Oliver Chang

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Executive Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

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

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd
June 2018

Copyright © 2018
Global Legal Group Ltd.
All rights reserved
No photocopying

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

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapters:

1	**The Rapid Evolution of Data Protection Laws** – Dr. Detlev Gabel & Tim Hickman, White & Case LLP		1
2	**Artificial Intelligence Policies in Japan** – Takashi Nakazaki, Anderson Mōri & Tomotsune		6

Country Question and Answer Chapters:

3	**Australia**	Holding Redlich: Trent Taylor & Daniel Clarkin	11
4	**Austria**	Herbst Kinsky Rechtsanwälte GmbH: Dr. Sonja Hebenstreit & Dr. Isabel Funk-Leisch	20
5	**Belgium**	Lydian: Bastiaan Bruyndonckx & Olivia Santantonio	30
6	**Brazil**	Vaz E Dias Advogados & Associados: José Carlos Vaz E Dias	41
7	**Canada**	Osler, Hoskin & Harcourt LLP: Adam Kardash & Patricia Kosseim	54
8	**Chile**	Rossi Asociados: Claudia Rossi	66
9	**China**	King & Wood Mallesons: Susan Ning & Han Wu	73
10	**Cyprus**	Koushos Korfiotis Papacharalambous LLC: Loizos Papacharalambous & Anastasios Kareklas	83
11	**France**	Clyde & Co: Benjamin Potier & Jean-Michel Reversac	93
12	**Germany**	GÖRG Partnerschaft von Rechtsanwälten mbB: Dr. Katharina Landes	103
13	**Hong Kong**	Ashurst Hong Kong: Joshua Cole & Hoi Tak Leung	113
14	**India**	Subramaniam & Associates (SNA): Hari Subramaniam & Aditi Subramaniam	126
15	**Isle of Man**	DQ Advocates Limited: Sinead O'Connor & Hazel Dawson	139
16	**Israel**	Naschitz, Brandes, Amir & Co., Advocates: Dalit Ben-Israel & Efrat Artzi	149
17	**Italy**	Trevisan & Cuonzo Avvocati: Julia Holden & Benedetta Marsicola	158
18	**Japan**	Mori Hamada & Matsumoto: Hiromi Hayashi & Rina Shimada	169
19	**Korea**	Lee & Ko: Kwang Bae Park & Hwan Kyoung Ko	179
20	**Luxembourg**	Loyens & Loeff Luxembourg S.à r.l.: Véronique Hoffeld & Florence D'Ath	188
21	**Macau**	Rato, Ling, Lei & Cortés – Advogados: Pedro Cortés & José Filipe Salreta	198
22	**Malta**	GANADO Advocates: Dr. Paul Micallef Grimaud & Dr. Philip Mifsud	208
23	**Mexico**	OLIVARES: Abraham Diaz & Gustavo Alcocer	218
24	**Netherlands**	Loyens & Loeff N.V.: Kim Lucassen & Iram Velji	226
25	**Nigeria**	Jackson, Etti & Edu: Ngozi Aderibigbe	238
26	**Norway**	Wikborg Rein Advokatfirma AS: Line Coll & Vilde Juliussen	248
27	**Portugal**	Cuatrecasas: Sónia Queiróz Vaz & Ana Costa Teixeira	260
28	**Romania**	Pachiu & Associates: Mihaela Cracea & Alexandru Lefter	272
29	**Senegal**	LPS L@w: Léon Patrice Sarr	282
30	**Singapore**	OrionW LLC: Winnie Chang	290
31	**Spain**	Ecija Abogados: Carlos Pérez Sanz & Pia Lestrade Dahms	299
32	**Sweden**	Affärsadvokaterna i Sverige AB: Mattias Lindberg & Marcus Lorentzon	310
33	**Switzerland**	Pestalozzi: Lorenza Ferrari Hofer & Michèle Burnier	320
34	**Taiwan**	KPMG Law Firm: Lawrence Ong & Kelvin Chung	330
35	**Turkey**	Fırat İzgi Attorney Partnership: Elvan Sevi Fırat & Doğukan Doru Alkan	338
36	**United Arab Emirates**	BSA Ahmad Bin Hezeem & Associates LLP: Rima Mrad & Nadim Bardawil	346
37	**United Kingdom**	White & Case LLP: Tim Hickman & Matthias Goetz	359
38	**USA**	Pillsbury Winthrop Shaw Pittman LLP: Deborah Thoren-Peden & Catherine D. Meyer	368
*	**Ireland**	Matheson: Anne-Marie Bohan (online only, see www.iclg.com)	

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

Disclaimer
This publication is for general information purposes only. It does not purport to provide comprehensive full legal or other advice.
Global Legal Group Ltd. and the contributors accept no responsibility for losses that may arise from reliance upon information contained in this publication.
This publication is intended to give an indication of legal issues upon which you may need advice. Full legal advice should be taken from a qualified professional when dealing with specific situations.

Sweden

Mattias Lindberg

Marcus Lorentzon

Affärsadvokaterna i Sverige AB

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The EU Regulation (EU) 2016/679 (the "**General Data Protection Regulation**" or "**GDPR**") will enter into force 25 May 2018. When in force, the GDPR will be the principal data protection legislation in the EU. Under the GDPR, the data protection legislation across the EU Member States will be more harmonised, though not in total since there are a lot of other data protection acts that still will be in force (e.g. covering areas such as healthcare and financial activities).

As a result of the GDPR, Sweden will get a new Data Protection Act ("**DPA**"). The new DPA will complement the GDPR in regard to the areas in which the GDPR opens up for national legislation.

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

The Camera Surveillance Act and the Electronic Communications Act implement the ePrivacy Directive 2002/58/EC. The European Convention on Human Rights has been incorporated into Swedish law which, primarily for the purpose of data protection, has an impact on the Swedish principle of openness (Sw. *offentlighetsprincipen*) and freedom of the press and freedom of speech (Sw. *tryck- och yttrandefriheten*).

The EU Commission has also proposed a new regulation on privacy and electronic communications that will apply to telecom and internet operators and replace the current Directive 2009/136/EC. The ePrivacy Regulation would harmonise the applicable rules across the EU.

The DPA authorises the government and the Swedish data protection authority, the Data Inspection Board ("**DIB**"), to issue more detailed regulations concerning several features of the DPA.

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

Hundreds of acts and ordinances contain regulations for registration and Processing of Personal Data, covering areas such as healthcare and financial activities.

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

According to the GDPR, it is mandatory for each EU Member State to provide for one or more supervisory authority/authorities to be responsible for monitoring the application of the GDPR. In Sweden, the Swedish data protection authority, the DIB, is responsible for the monitoring of the data protection legislation.

The DIB ensures that authorities, companies, organisations and individuals follow (i) the GDPR (as of 25 May 2018), (ii) the *old* Data Protection Act (until 24 May 2018), (iii) the Data Act, (iv) the Debt Recovery Act, and (v) the Credit Information Act.

The DIB works to prevent intrusion upon privacy through information and by issuing directives and codes of statutes. The DIB also handles complaints from individuals and organisations and carries out inspections. Inspections may be triggered by complaints but are normally planned and conducted in campaigns for sector-specific areas.

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.
- **"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 Subject"** means an individual who is the subject of the relevant Personal Data.
- **"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.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

- **"Processor"** means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller.
- **"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.
- **"Pseudonymisation"** means the Processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Data are not attributed to an identified or identifiable natural person.
- **"Consent"** of the Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

3 Territorial Scope

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

Yes, since the GDPR harmonises the data protection legislation across the EU Member States, some of the data protection laws apply to businesses outside of Sweden. All businesses that process Personal Data, either as a Controller or Processor, and that are established in any EU Member State, fall under the scope of the GDPR, regardless of whether or not the Processing takes place in the EU.

Furthermore, the GDPR applies to businesses that are established outside the EU, either if they are subject to the laws of an EU Member State or if they are Processing Personal Data of EU residents to be able offer goods or services or to monitor the behaviour of EU residents (if 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 in relation to the Data Subject. This means that the Controller must provide the Data Subject with certain minimum information, provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language, regarding the collection and Processing of the Personal Data.

- **Lawful basis for processing**

  It is only lawful to process Personal Data to the extent it is permitted under EU data protection law. According to the GDPR, Processing of Personal Data is permitted if: (i) the Data Subject has given Consent to the Processing of his or her Personal Data for one or more specific purposes; (ii) Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract; (iii) Processing is necessary for compliance with a legal obligation to which the Controller is subject; (iv) Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person; (v) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller; or (vi) Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the Data Subject is a child.

  Processing of sensitive Personal Data, such as data concerning health, political opinion or religious beliefs, require stronger legal grounds than regular Personal Data.

- **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. In certain cases, a Controller may use the relevant Personal Data in a manner that is incompatible with the purposes for which they were initially collected.

- **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.

- **Accuracy**

  Personal Data must be accurate and, where necessary, kept up to date, hence the Controller 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 Personal Data being processed; (iv) information about the categories of recipients with whom the Personal Data may be shared; (v) information about the period for which the Personal 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 restrict 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 Personal Data; and (ix) information about the existence of, and an explanation of

© Published and reproduced with kind permission by Global Legal Group Ltd, London

the logic involved in, any automated Processing that has a significant effect on the Data Subject.

- **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 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 Personal 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 Personal 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 Personal Data may only be held by the Controller, and may only be used for limited purposes if: (i) the accuracy of the Personal 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 Personal 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 right not to be subject to a decision based solely on automated processing**

  The Data Subject has the right not to be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

- **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 DIB, if the Data Subjects lives in Sweden or the alleged infringement occurred in Sweden.

- **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?

The Data Protection Directive 95/46/EC and the old DPA prescribed for a general obligation to notify Processing of Personal Data to the DIB. This obligation led to administrative and financial burden but did not always improve personal protection. Therefore, the GDPR does not contain any such obligations. Instead of the general obligation to notify the supervisory authority, the GDPR prescribes that the Controller shall perform a data protection impact assessment ("**DPIA**") or a prior consultation with the supervisory authority if the Processing is likely to, or would, result in a high risk to the rights and freedoms of natural persons.

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)?

A DPIA and a prior consultation with the supervisory authority may concern a single data Processing operation. However, a single assessment may address a set of similar Processing operations that present similar high risks.

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

DPIAs and prior consultations shall be made per data processing operation. Several Controllers may perform joint DPIAs and prior consultations.

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)?

If a Controller is established in more than one EU Member State or is carrying out cross-border Processing, the Controller may establish a lead supervisory authority that will handle all cases related to the Processing. Otherwise, the supervisory authority of the main or single establishment of the Controller is competent to be the supervisory authority.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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)?

A DPIA shall contain at least: (i) a systematic description of the envisaged Processing operations and the purposes of the Processing, including, where applicable, the legitimate interest pursued by the Controller; (ii) an assessment of the necessity and proportionality of the Processing operations in relation to the purposes; (iii) an assessment of the risks to the rights and freedoms of Data Subjects; and (iv) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data and to demonstrate compliance with the GDPR, taking into account the rights and legitimate interests of Data Subjects and other persons concerned.

A prior consultation with the supervisory authority shall contain: (i) where applicable, the respective responsibilities of the Controller, joint Controllers and Processors involved in the Processing, in particular for Processing within a group of undertakings; (ii) the purposes and means of the intended Processing; (iii) the measures and safeguards provided to protect the rights and freedoms of Data Subjects pursuant to the GDPR; (iv) where applicable, the contact details of the Data Protection Officer; (v) a DPIA; and (vi) any other information requested by the supervisory authority.

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

Non-compliance with a DPIA and prior consultation requirements can lead to fines of up to €10 million or 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

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

This is not applicable in Sweden.

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

This is not applicable in Sweden.

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

There is no such requirement in Sweden.

6.10 Can the registration/notification be completed online?

This is not applicable in Sweden.

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

There is no such list.

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

The supervisory authority shall, within a period of up to eight weeks from receipt of the request for consultation, provide written advice to the Controller.

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.

In some circumstances it is mandatory for Controllers and the Processors to appoint a Data Protection Officer. The most relevant circumstances being large-scale and systematic monitoring of individuals and/or large-scale Processing of sensitive Personal Data.

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

If the Controller or Processor fail to comply with a mandatory appointment of a Data Protection Officer, the Controller or Processor may be penalised with any penalties available under the GDPR.

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

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

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

Yes, provided that the Data Protection Officer is easily accessible from each establishment.

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

The Data Protection Officer should be appointed on the basis of professional qualities and should have an expert knowledge of data protection law and practices.

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

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 Personal Data of their obligations under the GDPR; (ii) monitoring compliance with the GDPR, national data protection legislation and internal policies in relation to the Processing of Personal Data including internal audits; (iii) advising on DPIAs and the training of staff; and (iv) co-operating with the data protection authority and acting as the authority's primary contact point for issues related to data Processing.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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

The Controller or Processor must notify the DIB of the contact details of the Data Protection Officer.

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

No. 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.

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, a Controller that appoints a Processor 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 and the obligations and rights of the Controller. To be able to fulfil the requirements of the GDPR, it is essential for the Controller to appoint a Processor that 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 Data Protection Officer; (vii) either returns or destroys the Personal Data at the end of the relationship (except as required by EU or Member State law); and (viii) provides the Controller with all the 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?)

The Marketing Act has regulations on marketing by email, fax or telephone. Under the Marketing Act, a trader may, in the course of marketing to a natural person, use email, a telefax or automatic calling device or any other similar automatic system for individual communication that is not operated by an individual, only if the natural person has Consented to this in advance. Where a trader has obtained details of a natural person's email address in the context of a sale of a product to that person, the Consent requirement shall not apply, provided that (i) the natural person has not objected to the use of the email address for the purpose of marketing via email, (ii) the marketing relates to the trader's own similar products, and (iii) the natural person is clearly and explicitly given the opportunity to object, simply and without charge, to the use of such details for marketing purposes, when they are collected and in conjunction with each subsequent marketing communication.

In marketing via email, the communication shall, at all times, contain a valid address to which the recipient can send a request that the marketing cease. This also applies to marketing to a legal person. A trader may use methods for individual marketing communication other than those referred to above, unless the natural person has clearly objected to the use of such methods.

According to the GDPR, the Data Subject shall have the right to object at any time to Processing of Personal Data concerning him or her for direct marketing purposes, which includes profiling to the extent that it is related to such direct marketing. Where the Data Subject objects to Processing for direct marketing purposes, the Personal Data shall no longer be processed for such purposes.

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.).

The Marketing Act prescribes that traders may use means of distance communication other than, for example, SMS and email, for marketing purposes unless the natural person clearly opposes the use of the method.

Good marketing practice requires marketers – before a call is made to a consumer in sales, marketing or fundraising purposes – to control if the consumer's phone number is in the blocking registry (NIX-Telefoni). The blocking registry is an opt-out registry which includes, from the year 2015, both regular phones and mobile phones. If a control is made, the company is entitled to call the consumer within two months from the day on which the used version of the track log was updated.

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

The Marketing Act applies to foreign companies provided that they target the marketing to a Swedish audience.

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

Yes, it is.

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

Yes, it is lawful. Marketers need to follow good marketing practice, which includes sector-specific ethical rules.

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

Breaches of the restrictions in the Marketing Act may result in a

© Published and reproduced with kind permission by Global Legal Group Ltd, London

penalty. In recent years, a standard of 5,000,000 Swedish kronor has been used. In addition, both traders and natural persons may claim damages.

Furthermore, traders may be ordered to pay a special charge (market disruption charge) if the trader, or a person acting on behalf of the trader, intentionally or negligently contravenes obligations in the Marketing Act. The market disruption charge shall be fixed at no less than 5,000 Swedish kronor and no more than 5,000,000 Swedish kronor. However, the charge may not exceed 10% of the trader's annual turnover.

10 Cookies

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

The Electronic Communications Act states that information may be stored in or retrieved from a subscriber's or user's terminal equipment only if subscribers or users are provided with access to information on the purpose of the Processing and Consents to the Processing. For Consent to be valid, it must be informed, specific, freely given and must constitute a real indication of the individual's wishes.

This does not apply to the storage or retrieval necessary for the transmission of an electronic message over an electronic communications network, or for the provision of a service explicitly requested by the subscriber or user.

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

The proposed rules will ensure that users get better control over their privacy settings and can easily Consent or deny cookies. According to the proposal, you do not need to Consent to the use of harmless cookies that make the site more user-friendly. For example, cookies that enable the service provider to remember what is in the customers "shopping cart" or to keep track of the number of visitors on a website will not require Consent.

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

Yes, the Swedish Post and Telecom Authority (Sw. "**PTS**") has carried out supervision in respect of the Processing of data and obtaining Consent in relation to cookies. The supervisions include how the companies obtain their respective Consent to use cookies. The PTS has thereafter produced a preliminary assessment based upon those supervisions on obtaining Consent in its endeavour for the general public to have greater insights and more influence over how personal information is used in connection with the use of telephones and the internet. A final assessment from the PTS will only be available in the respective decisions in regards to the supervisions of the respective companies. No such final assessments have been rendered yet. Hence, the preliminary standpoints are not binding but may nevertheless be indicative for companies who must observe the regulations on Consent in the Electronic Communications Act.

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

The penalty for breaches is a fine. The amount varies depending on the circumstances.

11 Restrictions on International Data Transfers

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

In principle, data transfers to jurisdictions outside of the European Economic Area (the "**EEA**") are not permitted. Data transfers to a jurisdiction outside the EEA can only take place if the Data Subject Consents to the transfer, if transfer is to an "Adequate Jurisdiction" or if the business has implemented one of the required safeguards as specified by the GDPR.

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

When transferring Personal Data to a country other than an Adequate Jurisdiction, businesses must ensure that there are appropriate safeguards on the data transfer, as prescribed by the GDPR.

For smaller businesses, the easiest way to comply with the data transfer rules is to get the Consent of the Data Subject or to carry out the data transfer as a result of the performance of a contract with the Data Subject.

For international businesses, data transfer to a jurisdiction outside of the EEA can be safeguarded by the implementation of Binding Corporate Rules ("**BCRs**"). The BCRs will always need approval from the relevant data protection authority.

Furthermore, businesses can adopt the Standard Contractual Clauses drafted by the EU Commission. The Standard Contractual Clauses are available for transfers between Controllers, and transfers between a Controller and a Processor.

Transfer of Personal Data to the US is also possible under the EU-US Privacy Shield Framework.

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.

Yes, most of the safeguards outlined in the GDPR will need initial approval from the DIB.

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.)?

Whistle-blowing hotlines are generally established in order to

© Published and reproduced with kind permission by Global Legal Group Ltd, London

implement proper corporate governance principles in the daily functioning of businesses. However, the company must comply with the fundamental requirements of the GDPR, and therefore have a legal ground; for example, for the Processing and provision of sufficient information to the Data Subjects.

The WP29 recommends that the business responsible for the whistle-blowing scheme should carefully assess whether it might be appropriate to limit the number of persons eligible for reporting alleged misconduct through the whistle-blowing scheme and whether it might be appropriate to limit the number of persons who may be reported through the scheme, in particular in the light of the seriousness of the alleged offences reported.

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

As there is no specific statute or guidance, anonymous reporting is not strictly prohibited or strongly discouraged under EU data protection law.

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 stages of the process, and in particular will not be disclosed to third parties, such as the incriminated person or 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.

13 CCTV

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

The Camera Surveillance Act regulates the use of equipment for audio-visual monitoring and surveillance. In general, permission is required for camera surveillance of sites to which the public has access, but sometimes a notification is sufficient.

From the data privacy perspective, a DIPA must be undertaken with assistance from the Data Protection Officer when there is 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 DIB.

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

CCTV monitoring may be used to prevent, investigate and reveal crimes, prevent accidents and other comparable purposes.

14 Employee Monitoring

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

Employee monitoring is subject to the general requirements of the DPA/GDPR. However, in the opinion of the DIB, employers cannot rely on Consent from employees to the Processing of Personal Data that occurs when an employee monitoring system is used. This is because employees often find themselves in a position of dependence upon their employers and are therefore unable to give the voluntary Consent required by the DPA/GDPR.

It has become more and more common for employers to use positioning systems of various kinds to check where their employees are.

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

Employers typically obtain Consent either by the employment agreement or by referencing the company's data protection policy. The employer can also justify its actions by a balance of interests in accordance with the DPA/GDPR.

It should be noted that in the opinion of the DIB, employers cannot rely on Consent from employees to the Processing of Personal Data. This is because employees often find themselves in a position of dependence upon their employers and are therefore unable to give the voluntary Consent demanded by the DPA/GDPR. Employers who want to use employee monitoring must normally rely on a balance of interests. The employer's interest in carrying out the Processing must then outweigh the employee's interest in protection from an invasion of privacy. In the overall assessment that must be performed in these cases, the following factors must be considered: (i) the purpose of the Processing; (ii) how the data are handled and how the results are used; (iii) what information is given to the employees; (iv) whether the Processing can be performed in a way that involves less invasion of privacy; (v) what technical and administrative security is available for the data; (vi) the existence of collective agreements and the content of these; and (vii) whether the Processing follows good practice for the labour market.

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

There is no absolute requirement to receive an approval from the relevant trade union. However, in the balance of interests in accordance with the DPA/GDPR, the opinion of the trade union may become an important factor. It is therefore important for the employer (and the Data Protection Officer) to have a good and productive relationship with the trade unions in the discussions of whether the Processing follows good practice for the labour market or not. Hence, it is normally well-invested time to initiate a discussion with the relevant trade union at an early stage in the process.

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, the Controller and Processor must ensure they have appropriate technical and organisational measures to meet the requirements of the GDPR. Depending on the security risk, this may include (i) the encryption of Personal Data, (ii) the ability to ensure the ongoing confidentiality, integrity and resilience of Processing systems, (iii) an ability to restore access to data following a technical or physical incident, and (iv) a process for regularly testing and evaluating the technical and organisation measures for ensuring the security of Processing.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

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.

Yes, 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 DIB, unless the breach is unlikely to result in a risk to the rights and freedoms of the Data Subjects. A Processor must notify any Data Breach to the Controller without undue delay, so that the Controller can report the Data Breach to the DIB.

The notification must include (i) the nature of the Personal Data Breach including the categories and number of Data Subjects concerned, (ii) contact details of the Data Protection Officer, (iii) the likely consequences of the breach, and (iv) 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 (i) the contact details of the Data Protection Officer, (ii) the likely consequences of the breach, and (iii) any measures taken to remedy or mitigate the breach.

Under some circumstances, the Controller may be exempt from notifying the Data Subject (e.g. if the risk of harm is remote or it the Controller has taken measures to minimise the risk).

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.

16 Enforcement and Sanctions

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

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
Investigative Powers	The data protection authority has wide powers to order the Controller and the Processor to provide any information it requires for the performance of its tasks, to conduct investigations in the form of data protection audits, to carry out reviews on certificates issued pursuant to the GDPR, to notify the Controller or Processor of alleged infringement of the GDPR, to access all Personal Data and all information necessary for the performance of Controllers' or Processors' tasks and access to the premises of the data including any data Processing equipment.	N/A
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
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 proceeding financial year.	N/A

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
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 proceeding financial year, whichever is higher.	N/A

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

The GDPR entitles the relevant data protection authority 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.

Consistent enforcement of the data protection rules is central to a harmonised data protection regime. The WP29 has created a document that is intended to ensure consistent application and enforcement of the GDPR. The powers described under question 16.1 will enter into force on 25 May 2018. Initially, the supervisory authorities are likely to use caution when exercising these powers.

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

Each supervisory authority shall ensure that the imposition of administrative fines pursuant to the GDPR. In case of cross-border Processing of Personal Data, the Controller shall establish a lead supervisory authority. However, the Data Subject may file a complaint to the local supervisory authority. The GDPR requires lead and concerned supervisory authorities to co-operate, with due respect for each other's views, to ensure a matter is investigated and resolved to each authority's satisfaction – and with an effective remedy for Data Subjects.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do companies typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

The concept of e-discovery does not exist in Sweden. However, the parties in civil cases under some circumstances have a duty of disclosure. There is no duty to disclose information to foreign law enforcement agencies.

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

There is no such guidance.

18 Trends and Developments

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

In Sweden, there is an extreme focus on integrity in both the strategic agreements and in GDPR projects as such. This trend is partly because of the new EU regulations but due to a large scandal, regarding the government's use of Personal Data and data security, during the summer of 2017.

The Swedish market is placing more and more focus on privacy issues in general by internally improving its processes in regards to quality. The DIB is encouraging entities to build privacy and data protection measures into the design of their data Processing in order to facilitate compliance with privacy and data protection principles. Hence, there is a lot of work going on so that authorities, companies, organisations and individuals will be able to meet the challenges resulting from the GDPR and the use of new technologies.

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

In general, the DIB is increasingly placing emphasis on the advice towards companies and organisations to conduct integrity analysis when taking important business decisions with regards to privacy issues.

The legislator is working hard to implement the data protection reform and update other registry legislation to function with the GDPR.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Mattias Lindberg
Affärsadvokaterna i Sverige AB
Västra Trädgårdsgatan 15
111 53 Stockholm
Sweden

Tel: *+46 708 13 05 18*
Email: *mattias.lindberg@affarsadvokaternasverige.se*
URL: *www.affarsadvokaternasverige.se*

Mattias Lindberg is the founding partner of Affärsadvokaterna i Sverige AB.

Mattias Lindberg has broad experience in providing legal advice and suggested measures in local and multi-jurisdictional outsourcing, strategic agreements, IT law and privacy law.

As a Data Privacy expert, Mattias Lindberg has extensive experience of analysing and implementing business-critical processes for the handling of personal data. He takes a methodical and pedagogic approach when analysing, optimising and implementing authority-regulated operational processes. As the personal data protection officer for several companies, Mattias Lindberg has extensive experience of implementing operational processes in accordance with the General Data Protection Regulation and the Patient Data Act.

Mattias Lindberg provides advice concerning all aspects of personal data management and regularly produces strategies regarding how personal data should be implemented and handled, and how integrity analysis should be conducted. Mattias Lindberg places particular focus on ensuring that the information is not only handled in accordance with the applicable laws and regulations, but that it is also handled in as practical and cost-effective a manner as possible. In addition, Mattias Lindberg has a great deal of experience in handling both ongoing contacts with the Data Inspection Board and audits conducted by the Board. He is also a highly-regarded public speaker, and is regularly invited to speak on various aspects of commercial law.

Marcus Lorentzon
Affärsadvokaterna i Sverige AB
Västra Trädgårdsgatan 15
111 53 Stockholm
Sweden

Tel: *+46 705 09 77 22*
Email: *marcus.lorentzon@affarsadvokaternasverige.se*
URL: *www.affarsadvokaternasverige.se*

Marcus Lorentzon is an associate at Affärsadvokaterna i Sverige AB.

Marcus Lorentzon has extensive experience within the fields of IT law and privacy law and provides advice concerning all aspects of privacy law. Marcus also holds experience of implementing operational processes in accordance with the General Data Protection Regulation and the Patient Data Act.

Furthermore, Marcus is specialised in tort and insurance law and has for several years worked within the insurance industry. Marcus is used to working with both the legal and commercial risks that companies face in their business and has good knowledge in managing and eliminating such risks.

AFFÄRSADVOKATERNA

Affärsadvokaterna is a modern firm focused on commercial law. Affärsadvokaterna offers legal services of the highest quality and with the greatest commitment. Affärsadvokaterna offers advice mainly in regards to strategic agreements, privacy law, IT law, outsourcing, dispute resolutions and procurements.

Affärsadvokaterna has a long history of providing advice in privacy law. Affärsadvokaterna provides advice to companies in privacy law issues, such as the production of information and agreements texts and the preparation of policy documents. Affärsadvokaterna has wide-ranging experience, and consequently an understanding of a company's special needs with regard to the processing of personal data in their specific business. Affärsadvokaterna has a methodical and pedagogic approach when authority-regulated operational processes are analysed, optimised and implemented. The clients appreciate the fact that the firm combines commitment and dedication with an in-depth understanding of the commercial and technical conditions of the industry. Its background as corporate lawyers combined with its legal experience gives Affärsadvokaterna the opportunity to offer clients focused and cost-efficient management of ongoing legal issues with industry expertise. As a result of the firm's extensive and broad knowledge, Affärsadvokaterna offers cutting-edge legal skills through a combination of commercial awareness, industry knowledge and legal expertise, which results in a business benefit for the client with regard to their use of personal data.

Affärsadvokaterna has a wealth of experience of analysing and implementing business-critical processes for the handling of personal data. The firm is appreciated by its clients for its long history in providing advice in privacy law. Affärsadvokaterna has a very strong focus on the healthcare and IT sector and is assisting both existing and new clients in regards to the General Data Protection Regulation.

Over the years, Affärsadvokaterna has also conducted its own specific examinations and integrity analysis of their clients' handling of personal data and other privacy-sensitive information. Affärsadvokaterna provides companies with tools, in the form of both projects and internal training, in order that, using an integrity analysis, they can analyse and continuously improve the processes that should be used in the challenge of cost-effectively complying with laws and regulations.

More information about cases and major accomplishments can be found at the website www.affarsadvokaternasverige.se.

© Published and reproduced with kind permission by Global Legal Group Ltd, London

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Cybersecurity
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- Franchise
- Gambling
- Insurance & Reinsurance
- International Arbitration
- Investor-State Arbitration
- Lending & Secured Finance
- Litigation & Dispute Resolution
- Merger Control
- Mergers & Acquisitions
- Mining Law
- Oil & Gas Regulation
- Outsourcing
- Patents
- Pharmaceutical Advertising
- Private Client
- Private Equity
- Product Liability
- Project Finance
- Public Investment Funds
- Public Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

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

www.iclg.com