ICLG

The International Comparative Legal Guide to:

Data Protection 2016

3rd Edition

A practical cross-border insight into data protection law

Published by Global Legal Group, with contributions from:

Affärsadvokaterna i Sverige AB
Bagus Enrico & Partners
Cuatrecasas, Gonçalves Pereira
Deloitte Albania Sh.p.k.
Dittmar & Indrenius
ECIJA ABOGADOS
Eversheds SA
Gilbert + Tobin
GRATA International Law Firm
Hamdan AlShamsi Lawyers & Legal Consultants
Herbst Kinsky Rechtsanwälte GmbH
Hogan Lovells BSTL, S.C.
Hunton & Williams
Lee and Li, Attorneys-at-Law
Matheson
Mori Hamada & Matsumoto
Osler, Hoskin & Harcourt LLP
Pachiu & Associates
Pestalozzi
Rossi Asociados
Subramaniam & Associates (SNA)
Wigley & Company
Wikborg, Rein & Co. Advokatfirma DA

global legal group

global legal group

Contributing Editor
Bridget Treacy,
Hunton & Williams

Sales Director
Florjan Osmani

Account Directors
Oliver Smith, Rory Smith

Sales Support Manager
Toni Hayward

Sub Editor
Hannah Yip

Senior Editor
Rachel Williams

Chief Operating Officer
Dror Levy

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.
April 2016

ISBN 978-1-910083-93-2
ISSN 2054-3786

Strategic Partners

MIX
Paper from responsible sources
FSC® C011748

General Chapter:

Country Question and Answer Chapters:

Sweden

Affärsadvokaterna i Sverige AB

Mattias Lindberg

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The prime legislation for Data Protection in Sweden is the Data Protection Act ("DPA"), which implements Directive 1995/46/EC.

Its primary goal is to guarantee that all individuals shall be protected against intrusions of their personal privacy, under the condition that such intrusions occur without their consent and involve the surveillance or systematic monitoring of the individual's personal circumstances.

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

The DPA authorises the government and the Swedish data protection authority, the Data Inspection Board ("DIB"), to issue more detailed regulations concerning several important features of the DPA. This authorisation has been relied on to issue the Data Protection Ordinance and several Regulations published by DIB.

The Camera Surveillance Act and the Electronic Communications Act are implementing 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 with regards to the Swedish principle of openness (Sw. *offentlighetsprincipen*) and freedom of the press and freedom of speech (Sw. *tryck- och yttrandefriheten*).

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 is the relevant data protection regulatory authority(ies)?

The task of DIB is to protect the individual's privacy in the information society without unnecessarily preventing or complicating the use of new technology. DIB ensures that authorities, companies, organisations and individuals follow (i) the DPA (1998), (ii) the Data Act (1973), (iii) the Debt Recovery Act (1974), and (iv) the Credit Information Act (1973).

DIB works to prevent intrusion upon privacy through information and by issuing directives and codes of statutes. 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"**

  All kinds of information that directly or indirectly may be referable to a natural person who is alive.
- **"Sensitive Personal Data"**

  Personal data relating to ethnicity, race, political or religious beliefs, trade union membership, health, sexual life and orientation, or actual or alleged criminal proceedings and convictions. Sensitive personal data are subject to increased compliance obligations due to their sensitive nature and the increased risk of harm to the individual if the data are improperly handled.
- **"Processing"**

  Any operation or set of operations which is taken with personal data, whether or not it occurs by automatic means, for example collection, recording, organisation, storage, adaptation or alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction.
- **"Data Controller"**

  A person who, alone or together with others, decides the purpose and means of processing personal data.
- **"Data Processor"**

  (Sw. "personal data assistant") a person who processes personal data on behalf of the controller of personal data.
- **"Data Subject"**

  (Sw. "the registered person") a person to whom the personal data relates.

- *Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data")*
  - **"Integrity Analysis"**

    To assess the risks for not keeping the integrity and protection of personal data as managed by the data controller's organisation.

3 Key Principles

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

- **Transparency**

  The controller of personal data shall ensure that a) personal data is processed only if it is lawful, b) personal data is always processed in a correct manner and in accordance with good practice, c) personal data is only collected for specific, explicitly stated and justified purposes, d) personal data is not processed for any purpose that is incompatible with that for which the information is collected, e) the personal data that is processed is adequate and relevant in relation to the purposes of the processing, f) no more personal data is processed than is necessary regarding the purposes of the processing, g) the personal data that is processed is correct and, if it is necessary, up to date, h) all reasonable measures are taken to correct, block or erase such personal data that is incorrect or incomplete regarding the purposes of the processing, and i) personal data is not kept for a longer period than what is necessary regarding the purpose of the processing.

- **Lawful basis for processing**

  For personal data to be processed lawfully, the data controller must have a legal basis for each processing activity.

  Personal data may be processed only if the registered person has given his/her consent to the processing or if the processing is necessary in order a) to fulfil a contract with the registered person or to enable measures that the registered person has requested to be taken before a contract is entered into, b) that the controller of personal data should be able to comply with a legal obligation, c) that the vital interests of the registered person should be protected, d) that a duty of public interest should be performed, e) that the controller of personal data or a third party to whom the personal data is provided should be able to perform a duty in conjunction with the exercise of official authority, or f) that a purpose that concerns a legitimate interest of the controller of personal data, or of such a third party to whom personal data is provided, should be able to be satisfied, given this interest is of greater weight than the interest of the registered person in protection against violation of personal integrity.

  Sensitive personal data may be processed for health and hospital care purposes, provided the processing is necessary for a) preventive medicine and healthcare, b) medical diagnosis, c) healthcare or treatment, or d) management of health and hospital care services.

- **Purpose limitation**

  The DPA states that the controller shall ensure that personal data is only collected for specific, explicitly stated and justified purposes.

- **Data minimisation**

  The controller of personal data shall ensure that (i) the personal data that is processed is adequate and relevant in relation to the purposes of the processing, and (ii) the personal data that is processed is correct and, if it is necessary, up to date.

- **Proportionality**

  The controller of personal data shall ensure that no more personal data is processed than is necessary regarding the purposes of the processing.

- **Retention**

  Personal data must not be retained for longer than is necessary for the processing purpose. Data controllers must ensure that data are only collected, used and retained to satisfy the relevant processing purpose. The DPA does not, however, stipulate any specific retention periods.

- *Other key principles – please specify*

  There are no other key principles in particular.

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 controller of personal data is liable to provide, to every natural person who requests it, a free-of-charge notification once a year of whether personal data concerning the applicant is processed or not. If such data is processed, written information shall also be provided about: (i) which information about the applicant that is processed; (ii) where this information has been collected; (iii) the purpose of the processing; and (iv) to which recipients or categories of recipients the information is disclosed.

  An application for information shall be made in writing to the controller and be signed by the applicant personally. The requested information shall be provided within one month from when the application was made. However, if there are special reasons for doing so, the information may be provided within four months from when the application was made.

- **Correction and deletion**

  The controller of personal data shall ensure that all reasonable measures are taken to correct, block or erase such personal data that is incorrect or incomplete with regards to the purposes of the processing.

- **Objection to processing**

  In those cases where processing of personal data is only permitted once the registered person has provided his/her consent, the registered person is at any time entitled to revoke his/her consent that has been given. Further personal data about the registered person, after this particular point in time, may not be processed.

- **Objection to marketing**

  Personal data may not be processed for purposes concerning direct marketing, provided the registered person gives notice in writing to the controller of personal data that he/she opposes such processing.

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

  Individuals may raise complaints with DIB.

- *Other key rights – please specify*

  There are no other key rights in particular.

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.)

Processing of personal data that is completely or partially automated is subject to a notification duty. The controller of personal data shall provide a written notification to DIB before such processing or a set of such processing with the same or similar purpose is conducted.

However, since there are several broad exemptions to the obligation to notify, notification is unusual in Sweden. Hence, registration is not required when, for example, (i) a personal data representative has been appointed, (ii) personal data is being processed in the context of 'unstructured material', (iii) personal data is processed by non-profit organisations with political, philosophical, religious or trade union objectives within the framework of their operations process where the data concerns the members of the organisation and such other persons who by reason of the objectives of the organisation have regular contact with, and (iv) personal data is processed under a sector-wide agreement which has been reviewed by DIB.

In addition, the DPA does not apply to such processing of personal data that a natural person performs in the course of activities of a purely private nature.

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

Registrations must be submitted for each legal entity. Each data controller that is under a duty to register must submit a registration which sets out its data processing activities.

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.)

The DPA applies to those controllers of personal data who are established in Sweden.

The DPA is also applicable when the controller of personal data is established in a third country but for the processing of the personal data uses equipment that is situated in Sweden. However, this does not apply if the equipment is only used to transfer information between a third country and another such country.

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 registration with DIB is done by submitting a notification form supplied by DIB. Notifications shall be made in writing and shall be signed by the data controller or its authorised representative. Notifications shall contain (i) the corporation's or organisation's name, address, telephone number and Swedish organisational registration number of the data controller, (ii) the purpose or purposes of the processing operation, (iii) a description of the category or categories of data subjects affected by the data processing, (iv) a description of the category or categories of data concerning the data subjects that are to be processed, (v) details of the recipients or categories of recipients to whom the data may be disclosed, (vi) information concerning any data transfer to third countries, and (vii) a general description of the measures that have been taken to ensure the integrity and protection of the personal data being processed.

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

A person who, intentionally or by recklessness, fails to register a notification where required, may be sentenced to imprisonment of six months at the most or, if the offence is grave, to imprisonment of two years at the most. A sentence shall not be imposed in petty cases. Data processors are not subject to the registration requirement.

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

There is no registration fee.

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

The registration/notification is valid indefinitely. If the controller of personal data has appointed a personal data representative, removal from office of the personal data representative shall also be notified to DIB.

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

Prior to the processing of personal data that involves particular risks for improper intrusion of personal integrity, such processing activities must be notified to DIB for an *ex ante* control. Such control means that DIB makes an assessment if the planned processing activities are in accordance with law. Such high-risk areas include some processing activities by the Swedish Tax Agency, the Swedish Customs and the Swedish Coast Guard.

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

A notification for preliminary examination shall be sent to DIB three weeks prior to the date on which the processing activities are planned to begin.

6 Appointment of a Data Protection Officer

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

It is not mandatory to appoint a Data Protection Officer.

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

This is not applicable.

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

If a personal data protection representative has been appointed (see question 6.4 below), such representative shall maintain a schedule of the processing that the controller performs and which would have been subject to the duty to given notice if the representative had not existed. Hence, voluntarily appointing a personal data protection representative is normally both time and cost efficient.

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

It is not mandatory to appoint a Data Protection Officer. However, it is very common to appoint a personal data protection representative. The personal data protection representative shall be a person, appointed by the controller of personal data, who shall independently ensure that the personal data is processed in a correct and lawful manner. There are no specific qualifications required for the personal data protection representative. The personal data protection representative may be an employee or a person, such as a lawyer, from outside the company.

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

It is not mandatory to appoint a Data Protection Officer but a personal data protection representative shall have the function of independently ensuring that the controller of personal data processes personal data in a lawful and correct manner and in accordance with good practice and also points out any inadequacies to him or her. If the personal data protection representative has reasons to suspect that the controller of personal data contravenes the provisions applicable for processing personal data, and if rectification is not implemented as soon as is practicable after being pointed out, the personal data protection representative shall notify this situation to DIB.

The personal data protection representative shall also otherwise consult with DIB in the event of doubt about how the rules applicable to the processing of personal data shall be applied.

The personal data protection representative shall maintain a register of all the processing that the controller of personal data implements and which would have been subject to the duty of notification if the representative had not existed.

The personal data protection representative shall assist registered persons to obtain rectification when there is reason to suspect that the personal data processed is incorrect or incomplete.

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

It is not mandatory to appoint a Data Protection Officer. However, if a personal data protection representative has been appointed, this must be registered/notified to DIB.

7 Marketing and Cookies

7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, email, 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 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.

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

Yes, it is.

7.3 Are companies required to screen against any "do not contact" list or registry?

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.

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

A trader 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.

The charge may not exceed 10 per cent of the trader's annual turnover.

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

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. 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.

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

It is stated in the preparatory works that Internet users should not be inconvenienced through cumbersome routines relating to the use of legitimate tools such as cookies. Hence, consent to cookies may therefore be expressed through web browser settings. However, it is not explicitly stated that browser settings are sufficient. A broad alliance of industry organisations and online international and domestic companies has collaborated on a code of conduct for cookie use.

7.7 To date, has 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 supervision includes approximately 10 companies of varying size and with different activities. The supervisions include how the companies obtain their respective consent to use cookies. PTS has thereafter produced a preliminary assessment based upon those supervisions on obtaining consent in its campaign 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 PTS will only be available in the respective decisions with 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.

7.8 What are the minimum penalties for breaches of applicable cookie restrictions?

There is no minimum penalty for breaches of applicable cookie restrictions but the maximum penalty for breaches is a fine.

8 Restrictions on International Data Transfers

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

Personal data may be transferred freely within EEA countries without restrictions. Since there are no general rules that provide corresponding guarantees outside the EU/EEA, it has been considered that transfers to such countries must be limited. Personal data may therefore only be transferred if there is an adequate level of protection in the recipient country or if there are special safeguards protecting the personal data and the rights of the data subjects.

Personal data may be transferred to a third country, for example when (i) there is an adequate level of protection in the recipient country, (ii) when the data subject has given his/her consent to the transfer, (iii) in certain specific situations enumerated in the DPA, and (iv) if it is permitted in some other way according to regulations or specific decisions by the Government or DIB with reference to that there are adequate safeguards with respect to the protection of the rights of the data subjects. Such safeguards may result from standard contractual clauses approved by the EU Commission or Binding Corporate Rules ("BCR").

The processing of personal data that takes place in Sweden must still comply with the DPA. This means that data may only be transferred if the data controller in Sweden has complied with the other requirements of the DPA; for instance, the fundamental requirements regarding processing of personal data and the rules for when such processing is permitted.

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

Companies normally (i) appoint a personal data representative, and (ii) perform an integrity analysis in order to assess the ways of protecting the integrity and quality of the personal data. A typical case is the use of cloud service suppliers.

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.

In principle, all personal data processing must be notified but there is a large number of exemptions from this rule. For example, a controller who has appointed a personal data representative within the company does not have to notify each instance of personal data processing. Furthermore, certain kinds of processing operations which are not likely to lead to privacy infringement do not have to be notified.

There is no requirement for a specific notification when personal data is to be transferred to a third country. However, the processing of personal data as such might have to be notified according to the DPA.

It is forbidden to transfer personal data to a non-EU country if the country does not have an adequate level of protection of personal data. All companies that transfer personal data outside the EU should evaluate whether the transfers are absolutely necessary, if it is possible to solve the need in another way than to transfer the personal data and the risks associated with the transfers and if there are legal and technical solutions to reduce the risks. Hence, a risk analysis shall be made. It can be noted that the European Court of Justice declared the old Safe Harbour framework invalid in its ruling on 6 October 2015. However, the EU Commission and the United States on 2 February 2016 agreed on a new framework for transatlantic data flows (the EU-US Privacy Shield) that will replace the old Safe Harbour framework. The new arrangement will include the following elements: (i) strong obligations on companies handling Europeans' personal data and robust enforcement; (ii)

clear safeguards and transparency obligations on U.S. government access; (iii) effective protection of EU citizens' rights with several redress possibilities; and (iv) annual joint review mechanism.

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.)

It is possible for companies to process personal data in whistle-blowing systems without having to apply for special permission from DIB. Companies that wish to create so-called whistle-blowing systems, where information about legal offences may be stated, must comply with the provisions of the DPA.

The company must comply with the fundamental requirements in the DPA, and therefore have a legal ground, for example, for the processing and provision of sufficient information to the data subjects.

The requirements in the DPA mean, among other things, that the reporting may only comprise serious improprieties committed by persons who have a key position or a leading position within their own company or group of companies.

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?

As there is no specific statute or guidance, anonymous reporting is not strictly prohibited or strongly discouraged under binding guidance.

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.

It is possible for companies to process personal data in whistle-blowing systems without having to apply for special permission from DIB.

9.4 Do corporate whistle-blower hotlines require a separate privacy notice?

The controller of personal data must, on his/her own initiative, provide information to employees or other persons whose data may be processed. No separate privacy notice is required, since such information can be provided as general information; for example, on a website providing all aspects of how to use the whistle-blower process.

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

The processing must not contravene with Swedish labour legislation or existing collective agreements and must be in compliance with good practices on the Swedish labour market. DIB has stated that processing of personal data in a whistle-blowing system can be permitted with a balancing of interest as ground. In such a balancing of interest, works councils/trade unions/employee representatives may be notified and/or consulted.

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)?

The Camera Surveillance Act regulates the use of equipment for audio-visual monitoring and surveillance.

In the opinion of DIB, the requirements of the DPA go beyond the demand for information concerning camera surveillance in the Camera Surveillance Act. In cases where the camera surveillance comprises the DPA, more effort is required than simply putting up signs in the spaces where the camera surveillance is carried out.

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

Employee monitoring is subject to the general requirements of the DPA. However, in the opinion of 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.

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

10.3 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.

It should be noted that in the opinion of 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. 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 is 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.

10.4 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, the opinion of the trade union may become an important factor. It is therefore important for the employer (and the personal data protection representative) to have a good and productive relationship with the trade unions in the discussions 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.

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

No, it does not.

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)?

Processing personal data in the cloud is permitted. DIB promotes the use of integrity analysis and has published a simple set of advice guidelines on data protection in cloud computing.

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)?

Whoever appoints a cloud provider is always the controller of personal data. Hence, the controller of personal data must: assess whether the processing of personal data that the cloud service provider is to carry out will be permitted under the DPA; carry out an integrity analysis in order to assess if it is possible to appoint the cloud service supplier for processing of the envisaged personal data, what security level is appropriate and what measures that have to be taken; ensure that there is a personal data processor agreement that meets the requirements of the DPA with the cloud provider; and be able to assure himself that all personal data processors actually take the security measures that are required.

If personal data comes to be processed by processors in a country outside the EU/EEA, the controller of personal data must ensure that one of the exemptions from the prohibition on transfer to a third country can be applied; for example when (i) there is an adequate level of protection in the recipient country, (ii) when the data subject has given his/her consent to the transfer, (iii) in certain specific situations enumerated in the DPA, and (iv) if it is permitted in some other way according to regulations or specific decisions by the Government or DIB with reference to the fact that there are adequate safeguards with respect to the protection of the rights of the data subjects. Such safeguards may result from standard contractual clauses approved by the EU Commission or Binding Corporate Rules ("BCR").

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)?

Big data and analytics are permitted. Where data are anonymous, the DPA does not apply.

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)?

The controller of personal data shall implement appropriate technical and organisational measures to protect the personal data that is processed. The measures shall provide a level of security that is appropriate regarding (i) the technical possibilities available, (ii) what it would cost to implement the measures, (iii) the integrity risks that exist with the processing of personal data, and (iv) the grade of sensitivity of the personal data being processed.

If the controller of personal data engages an external supplier of data services for systems containing personal data, the controller of personal data shall ensure for himself/herself that the supplier can implement the security measures that must be taken and ensure that the supplier actually takes the measures. DIB promotes the use of integrity analysis to define the risks, thus setting appropriate measures for security in level with the risks.

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.

There is no general notification requirement for data breaches in the DPA. DIB does not demand that such notification is done on the basis of general good practice.

However, the Health and Social Care Inspectorate (Sw. *Inspektionen för vård och omsorg* (*IVO*)) requires organisations to report data breaches and risks for loss of integrity of personal/patient data. In addition, the National Board of Health and Welfare (Sw. *Socialstyrelsen*) requires that caregivers once a year conduct an integrity analysis (Sw. *Patientsäkerhetsberättelse*).

In addition, there is a requirement in the Electronic Communications Act for providers of public electronic communications services to notify PTS (the Telecom supervising authority) in the case of privacy incidents. If the incident can be expected to have a negative effect for the subscribers and users concerned, or if PTS so requests, these subscribers and users must also be notified. Providers are required

to maintain an updated register over privacy incidents which their service has suffered. PTS has adopted supplementary regulations on notification of privacy incidents and published a guideline on the notification requirement.

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.

Individuals have the right to require rectification, blocking or erasing as applicable of such personal data that has not been processed in accordance with the DPA or regulations that have been made under the DPA. The controller must also notify a third party to whom the data has been disclosed about the measure, if the data subject requests it or if more substantial damage or inconvenience for the data subject could be avoided by a notification. However, no such notification needs be provided if it is shown to be impossible or would involve a disproportionate effort.

13.4 What are the maximum penalties for security breaches?

There are no penalties for security breaches but the DPA states that security breaches that lead to damage and violation of the personal privacy can lead to various damages.

14 Enforcement and Sanctions

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

Investigatory Power	Criminal/ Administrative Sanction	Criminal Sanction
Inspection matters which can involve requesting access to such personal data that is being processed.	Decision from DIB which can have an administrative fine.	This is not applicable.

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

DIB can sanction its decisions through an administrative fine. If DIB finds that a decision thus sanctioned has been breached, it cannot on its own authority enforce the administrative fine but has to seek a court order that the fine be paid. It is very uncommon that DIB seeks such enforcement.

DIB usually publishes its findings on their public website. The publicity in media normally provokes a fast response.

Only the Prosecution Authority can prosecute criminal offences under the DPA. Prosecution may be brought on the Prosecution Authority's own initiative or, following a complaint from DIB, from a perceived victim or from the general public.

15 E-discovery / Disclosure to Foreign Law Enforcement Agencies

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

The disclosure of personal data and the transfer of personal data are both processing activities requiring notice and a valid legal basis. Companies typically provide a general notice at the time of collection, e.g., stating in their privacy policies that the collected personal data may be disclosed in relation to legal proceedings or in response to law enforcement access requests.

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

DIB has not issued specific guidance on this issue.

16 Trends and Developments

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

The Swedish market is starting to prepare for the upcoming modernisation of the EU legal system for the protection of personal data so that authorities, companies, organisations and individuals will be able to meet the challenges resulting from the use of new technologies. Hence, 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. DIB has developed a checklist for IT projects and an information document that provides useful information with regards to privacy by design. DIB is also stressing the importance of updating policy documents and conducting integrity analysis. Entities are therefore placing more and more focus on privacy issues in general and updating policy documents, conducting integrity analysis and improving its processes with regards to quality in particular.

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

In general, 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. This said, more and more health and fitness services are emerging, which makes it possible to share and store a user's health information and even use open source code in apps and services. The focus on integrity analysis within the healthcare sector and for cloud services is therefore especially high.

In addition, and as described in more detail under question 8.3 above, there is much focus on the replacement of the old Safe Harbour framework with the EU-US Privacy Shield framework, and therefore, DIB has a focus on this new framework for transatlantic data flows.

As described under question 16.1 above, the new EU data protection reform is a legislative package that will update and modernise the data protection rules. DIB is raising awareness and will also deal with country specific topics with regards to the modernised rules.

Mattias Lindberg
Affärsadvokaterna i Sverige AB
Vildkattsvägen 1
167 66 Bromma
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 a broad experience in providing legal advice and suggested measures in local and multi-jurisdictional outsourcing, strategic agreements, IT law and privacy law.

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 representative for several companies, Mattias Lindberg has extensive experience of implementing operational processes in accordance with the Personal Data Act 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.

AFFÄRSADVOKATERNA

Affärsadvokaterna is a modern law firm focused on commercial law. The firm offers legal services of the highest quality and with the greatest commitment. Affärsadvokaterna offers advice concerning all kinds of strategic agreements, IT law, outsourcing and privacy law. Affärsadvokaterna also assists companies in business sales and acquisitions, as well as dispute resolution.

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. As a result of our 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 methodical and pedagogic approach when authority-regulated operational processes are analysed, optimised and implemented.

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.

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
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Franchise
- Gambling
- Insurance & Reinsurance
- International 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 Procurement
- Real Estate
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks

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