



Guidelines for companies

Responsibility for personal data processed in whistleblowing systems

FACTS

Personal Data Act

The Personal Data Act (PDA, 1998:204) entered into force in 1998 and its purpose is to protect people against infringement of their privacy through the processing of personal data. The Personal Data Act is based on common rules adopted within the EU, the so-called Data Protection Directive. Consequently, other EU-countries have similar protective legislation.

Controller of personal data

The controller of personal data is normally the legal person (for example a joint-stock company, foundation or association) or the public authority that processes personal data in its activities and that decides which data to process and for what the data will be used. Thus it is not the employer of a place of work or an employee who is the controller of personal data.

Data Privacy Officer

The controller of personal data may appoint a data privacy officer who shall ensure that the personal data is processed in a correct and lawful manner within the establishment. The privacy officer shall maintain a register of the processing carried out and assist data subjects to obtain rectification if the data is incorrect. More than 6 100 establishments have notified representatives (January 2009).

Guidelines for companies

Responsibility for personal data processed in whistleblowing systems

October 2010

Contents

- Summary 4
- Background to the regulation 5
- This is the meaning of the regulation. 6
- The company is responsible. 7
- The requirements in both the Personal Data Act
and the regulation must be fulfilled 7
- The requirements in the Personal Data Act
on the whistleblowing system 8
- Fundamental requirements must be fulfilled 8
- Balance of interest 8
- Sensitive personal data requires specific grounds 9
- The data subjects must be informed 9
- Security measures shall protect the personal data 10
- If personal data is transferred outside the EU 10
- The requirements in the regulation on the whistleblowing system ... 11
- Authorization is required if the regulation is not complied with 12
- If the rules are not complied with. 12

Summary

Through a new provision in the **Data Inspection Board Statute Book DIFS 2010:1** it is now possible for companies to process personal data in whistleblowing systems without having to apply for a special permission from the Data Inspection Board.

However, the same substantial conditions as before are applicable to such systems. Companies that wish to create so-called whistleblowing systems, where information about legal offences may occur, must comply with the provisions of the Personal Data Act (PDA), and the specific prerequisites described in the new regulation.

The requirements in the Personal Data Act imply among other things that the company must comply with the fundamental requirements in the Personal Data Act, have a legal ground for the processing and provide sufficient information to the data subjects.

The requirements in the regulation 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 the own company or group of companies.

FACTS

What is a whistleblowing system?

There is no general definition of the notion whistleblowing. The Data Inspection Board is of the opinion that the notion comprises specific channels for reporting set up with the aim of facilitating for employees to report suspected crimes against the company's own code of conduct as well as against national law. Such channels for reporting can be a special e-mail address, a telephone service or a website through which information about suspicions of crimes regarding individual persons is collected and processed. In a group of companies the information does not always remain within the company where the reported person is employed but is forwarded within the group of companies.

Background to the regulation

Many companies provide for special reporting channels that employees can use to report serious improprieties within the companies, for example accountancy crimes or bribery crimes. The requirements that companies should have such a reporting channel originate principally from the US and from the American stock exchanges where this type of systems is called whistleblowing systems.

According to Section 21 in the Personal Data Act (1998:204) it is prohibited for other parties than public authorities to process personal data concerning legal offences. The Data Inspection Board may, however, decide on an exemption from this prohibition, either through individual decisions or in general regulations.

Since 2008 a large number of companies have applied for and been granted an exemption from Section 21 in the Personal Data Act to process personal data concerning legal offences in whistleblowing systems. In order to facilitate the companies' handling and at the same time maintain the requirements set up for the protection of privacy the Data Inspection Board has now issued a general regulation (DIFS 2010:1) that makes it possible, under certain conditions, to process such information without a special decision from the Data Inspection Board.

These guidelines describe which rules that are to be applied for such processing of personal data.

The so-called Article 29 Working Party (a working group consisting of representatives of all data protection authorities of the EU-countries) has also given its opinion as regards what ought to apply to whistleblowing systems in the light of the rules of the EU Data Protection Directive. The opinion (WP 117) is available on the EU Commission's website on data protection.

This is the meaning of the regulation

The use of a whistleblowing system involves processing of personal data within the meaning of the Personal Data Act. The Data Inspection Board has found that this is a case of such structured processing of personal data that falls under the rules of the Personal Data Act. This means that the controller of personal data does not have the possibility to apply Section 5 a of the Personal Data Act.

Information about that someone has committed or may have committed a crime constitutes information about a legal offence even if there is no judgment or anything corresponding concerning the crime. According to Section 21 of the Personal Data Act it is prohibited for other parties than public authorities to process personal data concerning legal offences involving crime, judgments in criminal cases, coercive penal procedural measures or administrative deprivation of liberty. The prohibition applies even if the data subject would consent to the processing.

Notwithstanding the prohibition in Section 21 of the Personal Data Act special situations may occur when it is legitimate for companies to process such personal data. According to Section 9 of the Personal Data Ordinance (1998:1191) the Data Inspection Board may issue regulations about exemptions from the prohibition. The Data Inspection Board may also decide on exemptions from the prohibition in individual cases. The exemptions that the Inspection has issued earlier in the regulation DIFS 1998:3 have been considered not to be valid for whistleblowing systems. Therefore, the Data Inspection Board has instead, after an application, rendered special decisions on exemptions in individual cases. The regulation has now been amended. A new provision has been introduced in point f) that deals with processing of crime information in whistleblowing systems. The new provision applies as of 1 November 2010. The amendment appears from DIFS 2010:1.

The new regulation means that companies that wish to process personal data in whistleblowing systems do not any longer have to apply for a specific exemption from Section 21 of the Personal Data Act. This does not imply any change in substance as regards the handling of information in whistleblowing systems. The regulation contains the same requirements as the Data Inspection Board earlier laid down in its decisions on exemptions from the prohibition and all the Personal Data Act's provisions must be observed in the processing.

As regards companies that have already been granted an exemption the regulation does not imply any change. They may continue processing data in the same manner as earlier in accordance with the decisions issued.

The company is responsible

A person who alone or together with others decides the purposes and means of processing personal data is the controller of personal data in the meaning of the Personal Data Act (Section 3 of the Personal Data Act).

The Data Inspection Board considers that each company is responsible for the collection and disclosure of personal data that may occur as the company gives its employees and others the possibility to use a whistleblowing system. By providing and assigning the reporting channels mentioned to its employees the company is considered to decide the purposes and means for the collection of personal data. This is true even if the data finally would end up in another company of the group, for example the mother company. The company is also responsible for the continued processing of personal data that the company may carry out as regards the information given. This does not exclude that also other companies of the group may be responsible for the same personal data.

An external party is often engaged to receive the reports in a first phase. Such an external party is to be considered as processor of personal data and may only process the data in accordance with instructions from the controller of personal data (Section 30 of the Personal Data Act). There is also a requirement for a written contract, see more under the heading *Security measures shall protect the personal data*.

The requirements in both the Personal Data Act and the regulation must be fulfilled

When processing personal data in a whistleblowing system the controller of personal data must comply with:

- relevant provisions in the Personal Data Act
- the requirements in the regulation

The requirements in the Personal Data Act on the whistleblowing system

Fundamental requirements must be fulfilled

In the Personal Data Act there are fundamental requirements that always have to be complied with in order that personal data may be processed (Section 9 of the Personal Data Act). For whistleblowing systems these requirements imply among other things the following :

- The processing must not contravene Swedish labour legislation or existing collective agreements.
- The processing must be in compliance with good practices on the Swedish labour market.
- The system must be set up in a way that does not lead to the risk that more personal data is processed than is necessary or relevant having regard to the purpose of the processing, or that sensitive data is processed in contravention of the Personal Data Act. This can be done through explicit directions for users, training, technical restrictions and sufficient security measures.
- Data that is collected and stored must be correct, adequate and relevant. This means that the company promptly may have to make a first check and assessment of the received data.
- Data may not be kept for a longer period than that as is necessary having regard to the purpose of the processing. A report that is found to be ungrounded should be deleted immediately. If a report leads to an investigation the data should be deleted when the investigation is completed or, if the investigation leads to measures being taken in relation to the data subject, when the data no longer is needed for this purpose.

Balance of interest

A controller of personal data may only process personal data if the data subject has given his/her consent to the processing or if the processing is necessary for certain purposes (Section 10 of the Personal Data Act). Such a purpose is, for example, that the controller of personal data should be able to comply with a legal obligation. This means in the first place an obligation based on Swedish rules or EU-legal provisions.

Personal data may be processed without consent after a balancing of interest, that is to say if the controller of personal data has a legitimate

interest to process the personal data and this interest is of greater weight than the interest of the data subject in protection against violation of privacy.

The Data Inspection Board considers that processing of personal data in a whistleblowing system can be permitted with such a balancing of interest as ground. In this balancing regard has been paid to possible obligations in foreign legislation, such as the Sarbanes-Oxley rules in the US, but a legitimate interest can also be at hand as regards companies that are not subject to such rules.

Sensitive personal data requires specific grounds

Personal data that according to the Personal Data Act is sensitive, for example data revealing ethnic origin, political opinions, religious belief or that concerns health and sexual life may only be processed under certain conditions (Sections 15–19 of the Personal Data Act). The system for whistleblowing must be set up in such a way that the risk of processing sensitive personal data in contravention of the Personal Data Act is minimized.

The data subjects must be informed

The controller of personal data must on his/her own initiative provide information to employees or other persons whose data may be processed (Sections 23–25 of the Personal Data Act). Such information can be provided as general information, for example on the website where information about the reporting channels has been collected.

The information should comprise data about:

- the identity of the controller of personal data as well as his/her contact details
- the purpose of the processing
- what kind of data that is being processed
- that it is voluntary to make a report via the specific reporting channels
- to what categories of recipients the information might be disclosed
- that the data subject has the right to request an excerpt of the register to check which information if any that is registered about him or her and

- that the controller of personal data is liable at the request of the data subject to rectify personal data that is incorrect, incomplete or misleading.

When data has been collected, the data subject shall also receive specific information thereof. If it is not possible to provide such information at once, for instance because it could jeopardize the subsequent investigation, you can wait with the information to the data subject until there is no such risk any longer. However, the data subject shall be informed as soon as possible and at the latest in conjunction with the data being used in order to take measures concerning him or her.

Information must also be provided to anyone who requests to know whether there is data registered about him/her (Section 26 of the Personal Data Act). Such information shall be provided within one month and at the very latest within four months from when the application was made. However, the information must not disclose the identity of the person who made the report.

A company may refuse to provide information to the data subject in a corresponding case as referred to in the Publicity- and Secrecy Act (2009:400) – (Section 27 of the Personal Data Act).

Security measures shall protect the personal data

The controller of personal data shall implement appropriate technical and organisational security measures to protect the personal data (Sections 30–31 of the Personal Data Act). The handling of the personal data shall be restricted solely to those persons who handle reports and investigate suspected improprieties. If a processor is engaged to process the data on behalf of the controller of personal data there shall be a written contract which specifically stipulates that the processor may only process the data in accordance with instructions from the controller of personal data and that the processor is liable to take those measures referred to in Section 31 of the Personal Data Act. For more information about security, see the Data Inspection Board's general advice *Security for personal data* from November 2008 which is accessible via the Data Inspection Board's website, www.datainspektionen.se.

If personal data is transferred outside the EU

If personal data is transferred to a third country there are more requirements. If data is sent to someone established outside the EU, for instance another company within the group or a processor of personal data, the rules in the Personal Data Act about such transfers must be complied with (Sections 33–35 of the Personal Data Act). This means

among other things that the third country in which the recipient is must be approved by the Commission as a country with an adequate level of protection or that the transfer is regulated in an agreement containing such standard contractual clauses that the Commission has approved as offering sufficient safeguards. For more information about transfers to third countries, see www.datainspektionen.se/in-english/in-focus-transfer-of-personal-data

The requirements in the regulation on the whistleblowing system

In a whistleblowing system privacy sensitive information is processed. In order for such processing of personal data to be permitted with a balancing of interest as ground the controller of personal data must be able to adduce weighty arguments. Therefore a whistleblowing system should only be used for such improprieties that may result in serious consequences for the company.

Therefore the following restrictions apply to whistleblowing systems:

- Processing of personal data concerning legal offences may only refer to persons in key positions or a leading position within the own company or group.
- Data may only be processed in the system if it is objectively justified to process the data in order to investigate if the person in question has been accessory in serious improprieties.
- The processing may only refer to data about serious improprieties concerning:
 - accounting, internal accounting controls, auditing matters, fight against bribery, banking- and financial crime, or
 - other serious improprieties concerning the company's or the group's vital interests or the life or health of individual persons, as for instance serious environmental crimes, major deficiencies as regards the security at the place of work and very serious forms of discrimination or harassments.

Three of the previous decisions of the Data Inspection Board in individual cases have been appealed against with regard to the restriction under the first point. The Administrative Court rejected the appeals. See for instance *Judgment of the Stockholm Administrative Court 2010-03-12, case nr 12584-10*.

The meaning of that data may only be processed in the system when it is objectively justified is clearly stated in the previous decisions of the Data Inspection Board and is still valid. The system may only be used when it is objectively justified not to use the company's internal information- and reporting channels, for instance if the reported person is part of the management and the suspected improprieties for that reason otherwise run the risk of not being properly handled. This also means that the system shall constitute a complement to normal internal administration and must be voluntary to use.

Authorization is required if the regulation is not complied with

The possibility to process personal data concerning legal offences without having to apply for authorization from the Data Inspection Board only applies if you comply with one of the general regulations of the DIFS 2010:1. If you wish to process such data in any other manner you must apply for a special exemption from the Data Inspection Board.

In order to process other personal data than information concerning legal offences there is no requirement for a decision from the Data Inspection Board, but the controller of personal data is always responsible to see to that the rules in the Personal Data Act are complied with.

If the rules are not complied with

To process personal data in contravention of the rules in the Personal Data Act (including Section 21 of the Personal Data Act) is punishable (Section 49 of the Personal Data Act). The data subject has also a right to damages for harm and infringement of privacy caused by the fact that personal data has been processed in contravention of the Personal Data Act (Section 48 of the Personal Data Act).

The Data Inspection Board has the task to supervise the processing of personal data that occurs. This can be done either through on-site inspections or through written contacts. The powers of the Data Inspection Board are stated in Sections 43-47 of the Personal Data Act.

Contact the Data Inspection Board

E-mail: datainspektionen@datainspektionen.se Website: www.datainspektionen.se
Telephone +46 (0) 8 657 61 00. Postal address: Datainspektionen, Box 8114, SE 104 20 Stockholm



Data Inspection Board