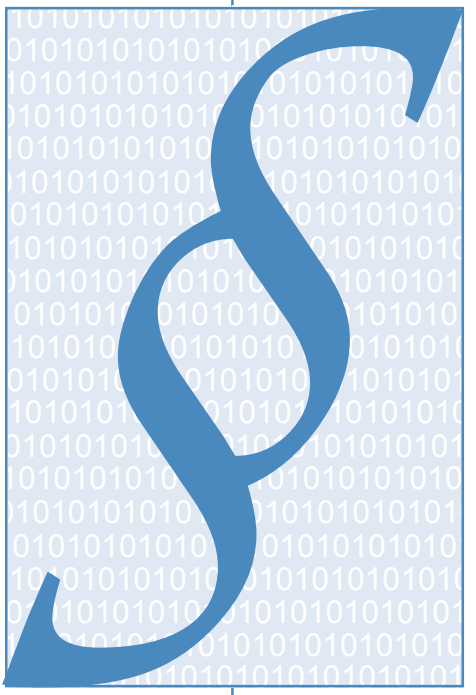
Personal Data Protection



Information on the Personal Data Act

REGERINGSKANSLIET

Personal Data Protection

Information on the Personal Data Act

Other publications in this series are:

Copyright
Family law – Information on the rules
Public access to Information and secrecy with Swedish Authorities

This brochure is produced by the Ministry of Justice.
Additional copies can be ordered from
the Ministry of Justice, SE-103 33 Stockholm
Fax: 08-20 27 34
Internet: www.sweden.gov.se

Large orders (10 copies or more):

Fritzes kundtjänst
SE-106 47 Stockholm
Fax +46 8 690 91 91
Tel. +46 8 690 91 90
Internet: www.fritzes.se
ISBN 91-38-31558-0
4th revised edition 2006

Foreword

On 24 October 1998, a new act entered into force aimed at preventing the violation of personal integrity by the processing of personal data, namely the Personal Data Act (SFS 1998:204). This Act is based on common rules decided within the EU.

The Government has issued supplementary regulations in conjunction with the Act in the Personal Data Ordinance (1998:1191).

The Data Act (1973) is repealed by the Personal Data Act.

This brochure provides an overall presentation of the Personal Data Act.

Amendments to the Act have been taken into account up to SFS 2006:398. This brochure presents the Act in its wording from 1 January 2007. Readers wishing to learn more about the Act may read the Government Bills 1997/98:44, 1999/2000:11 and 2005/06:173 together with the Standing Committee on the Constitution Report 1997/98:KU18. The first Bill referred to reports, inter alia, on the underlying EU rules. This material is also available on the Internet: *www.riksdagen.se/dokument*.

Further information is included in the report presented by the Data Law Commission in March 1997 and which formed the basis for the new Act: Integrity – Public Access to Information – Information Technology (Official Government Report SOU 1997:39). In addition, information about the application of the Act is available in the report presented by the Personal Data Commission in January 2004 which served as the basis for the most recent amendments to the Act: Review of the Personal Data Act (Official Government Report SOU 2004:6).

The Data Inspection Board is the supervisory authority under the Personal Data Act and may, in that capacity, provide information about the rules. Information is also available on the Board's website on the Internet: *www.datainspektionen.se*

Stockholm, October 2006

Contents

1 Background to the Personal Data Act

Developments within information technology are accelerating. Technology becomes increasingly powerful, simpler to use and less expensive. This means that it is available to increasing numbers of people. At the same time, it is becoming easier to receive and disseminate data stored on the computer. The facilities for storage and searching for information are becoming increasingly flexible.

The opportunities afforded by new technology have brought with them an increase in the amount of data connected to people, for example, with the use of computers. Awareness has also increased that more and more data is available from an increasing number of sources. The methods that have been used to gather and process data relating to people are being continuously refined. A person using the Internet or modern cards for, for example, payment, can readily – without being aware of the fact – leave a so-called electronic trail behind him/herself.

Developments have meant that technology can be used in a manner that involves an unacceptable intrusion into personal integrity. The individual is entitled to be protected by society against such violations of integrity. At the same time, the need of the individual for protection must be balanced against other fundamental democratic rights and values, for example, freedom of information and freedom of expression. Legitimate needs for using information related to people also exist, for example, for the purpose of social planning.

A considerable amount of balancing is thus necessary when formulating legislation to protect personal integrity as regards personal data. Furthermore, the legislation must not unnecessarily restrict the use of new technology. New technology brings with it not only risks but also advantages. Things that were not previously feasible are now possible thanks to new technology – something which has already involved an improvement in the standard of living and increased freedom for many people.

The Swedish Data Act (1973) has been considered to be outdated for many years. It has not corresponded in all respects with the standards that can be expected for legislation to effectively protect personal integrity. The Data Act therefore needed to be replaced by a new modern Act. The rules have been

developed having regard to the Data Protection Directive that was adopted by the EU in 1995 which is now introduced in all Member States. A basic starting point has been that responsibility for ensuring that personal data is conducted in a lawful manner should rest with the person processing such data.

2 What does the Personal Data Act mean?

The main features of the Personal Data Act are presented in this part. These are:

- People shall be protected against the violation of their personal integrity by processing of personal data.
- In contrast with the Data Act, the Personal Data Act does not only apply to automated processing of personal data but, in certain cases, also to manual registers.
- The Personal Data Act does not apply to the processing of personal data that forms part of a course of operation of a purely private nature.
- The provisions of the Act are not applicable to the extent that they would contravene the constitutional provisions relating to freedom of the press and freedom of expression or limit the principle of access to public information.
- The Act does not apply, in principle, to journalistic, artistic or literary activities
- Processing of personal data in unstructured material, for example running text, may take place as long as this processing does not entail a violation of the registered person's personal integrity. Most of the other provisions of the Act shall not be applied to processing of this kind.
- If another act or ordinance contains rules that deviate from the Personal Data Act, those other provisions apply instead.
- The old system with licences and permits is abolished. Responsibility for ensuring that processing of personal data is conducted in a lawful manner is imposed in the first instance, upon the person processing such data. The Data Inspection Board exercises supervision of compliance with the Personal Data Act.
- The Personal Data Act lists certain fundamental requirements concerning the processing of personal data. These demands include, inter alia, that personal data may only be processed for specific, explicitly stated and justified purposes.
- Personal data may, if these fundamental requirements are satisfied, in principle, only be processed if the registered person gives his or her consent. Howe-

ver, there are several exceptions to this rule, for example, if it is necessary
– in the exercise of official powers
– when a work task of public importance is to be performed
– in order to enable the controller of public data to fulfil a legal obligation
– in order that a contract with the registered person may be performed.

- Particularly stringent rules apply to the processing of sensitive personal data – e.g. concerning political views or health. These rules also apply to the transfer of personal data to other countries.
- The registered person is entitled to information concerning processing of personal data that concerns him/her.
- The processing of personal data shall be notified to the Data Inspection Board. However, this does not apply if the person who is responsible for the processing has appointed a personal data representative.
- A person who contravenes the Personal Data Act may be liable to pay damages or be sentenced to a criminal penalty.

3 The terminology of the Personal Data Act

The Personal Data Act uses some central concepts that reappear at several places in the various connections, inter alia in this brochure, and which are therefore useful to know. The most important of them are presented below.

3.1 Personal data

All kinds of information that is directly or indirectly referable to a natural person who is alive constitute personal data.
The Personal Data Act applies to such processing of personal data as is wholly or partly performed with the aid of computers. The Act also applies to other processing of personal data, if these form part of or are intended to form part of a structured collection of personal data that is available to searches or compilations according to specific criteria (so-called manual registers).

The Act does not apply to the processing of personal information that a natural person performs in an activity of a private nature. This means, for example, that individuals may maintain for purely private use electronic diaries or a register of the addresses of friends and relatives etc. The word and text processing and communication by electronic mail of individuals also normally fall outside the ambit of the Act.

A simplified provision applies to processing of personal data in unstructured material, for example, running text, stipulating that the processing may not entail a violation of the personal integrity of the registered person (see Part 6).

3.2 Processing (of personal data)

Processing means everything one does with personal data, whether performed through a computer or not. The following may be mentioned as examples of processing of personal data

- Collection
- Registration
- Storage
- Processing

- Disclosure by transfer, dissemination or other provision of data
- Compilations or joint processing.

There is no requirement that the information processed as data should be structured in a register or the like. Computerised work and text processing or similar processing of running text containing personal data is therefore per se subject to the Act, although a simplified provision applies to processing personal data in unstructured material, for example, running text (see Part 6).

Personal data in structured material may only be processed for specific, explicitly stated purposes.

Data that one has gathered for a particular purpose may not later be processed in a manner that is not compatible with that purpose.

3.3 The controller of personal data and the personal data assistant

A person who alone or together with others decides why and how personal data shall be processed is called the controller of personal data (the controller). This is usually a legal person – a company, an association, a public authority or a local authority. A natural person – for instance, a businessman – may also be a controller, however.

Personal data assistant (assistant) means a person who processes personal data on behalf of the controller. The assistant may be an independent service provider.

3.4 Personal data representative

A personal data representative (representative) is a natural person who, on the assignment of the controller, shall ensure that personal data is processed in a lawful and proper manner.

The representative must point out any inadequacies for the controller.

If the representative has reason to suspect that the controller is contravening the provisions applicable to the processing of personal data, and points this out, but the controller does not rectify the matter as soon as practicable, the representative must notify this to the Data Inspection Board.

The representative shall also liaise generally with the Data Inspection Board if doubt prevails concerning whom the provisions applicable to processing of personal data should apply to. The representative shall also assist the registered person to obtain rectification if there is reason to suspect that personal data processed is incorrect or incomplete. Furthermore, the 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 (cf Part 14).

The appointment and removal from office of a representative must be notified to the Data Inspection Board.

3.5 Consent

Consent means every kind of voluntary, specific and unambiguous expression of will, by which the registered person, after the receipt of information, accepts the processing of personal data concerning him/her.

Consent may either be verbal or in writing. It must be voluntary.

The registered person must, before consent is given, have received the information necessary to enable him/her to assess the advantages and disadvantages of the processing of the personal data concerned and so that he/she may exercise his/her rights under the Personal Data Act. Consent shall also be unambiguous. Thus, no doubt may prevail about whether voluntary consent has been given. The consent must also be specific, which means that it must apply to a particular processing concerning the registered person that is performed by a particular controller for a particular purpose.

4 The scope of the Personal Data Act

The Personal Data Act applies to those controllers who are established in Sweden. As a main rule, Swedish law is also applicable when a controller from a third country (i.e. a country outside the EU and EEA) uses equipment, for example terminals and questionnaires, situated in Sweden for the processing of personal data. In such cases, the controller must appoint for himself an agent who is established in Sweden. The agent is equated with a controller when applying the Personal Data Act.

The Personal Data Act never applies if equipment is only used to transfer information between two countries that are outside the EU and EEA.

5 The principle of public access to official documents and also freedom of the press and expression

The principle of public access to official documents, which is embodied in the Freedom of the Press Act means that the public authorities are liable upon request to provide copies of public documents unless secrecy applies. The duties of public authorities to save information – and not to alter it in such a manner as the original information is erased – is also of importance to the principle of public access to official documents.

The provisions of the Personal Data Act are not applied in such a manner that they might limit the principle of public access to documents or contravene the provisions concerning the freedom of the press and freedom of expression contained in the Freedom of the Press Act or Fundamental Law on Freedom of Expression.

The Personal Data Act also includes an exemption for such processing of personal data as is only related to journalistic work or artistic or literary creation. However, the provisions of the Act concerning security measures when processing personal data (see Part 12) shall be applied in such cases.

6 Personal data in unstructured material

The great majority of provisions of the Personal Data Act need not be applied when processing personal data in unstructured material, for example, running text. This may entail sound or images, e-mail messages, texts published on the Internet or short or long memoranda or other documents produced with word processing software. In order for the simplified regulation to apply, the material worked with must not be included in or be intended to be included in a document or case management system or any other database. The provisions of the Act on security measures when processing personal data (see Part 12) must also be applied. However, it is not necessary to apply the provisions on fundamental requirements for processing personal data (Part 7), permitted processing of personal data (Part 8), information to the person who is registered (Part 9) and transfer of personal data to a third country (Part 13).

Processing of personal data in unstructured material must not, however, entail a violation of the integrity of the registered person. The following guidelines should be complied with:

- Do not process personal data for improper ends, such as persecution or disgracing.
- Do not compile a large quantity of data about one person without acceptable reason.
- Correct personal data which proves to be incorrect or misleading.
- Do not defame or insult another person.
- Do not breach secrecy or a duty of confidentiality.

In the first place, it is the responsibility of the controller to ensure that no violation takes place in particular cases. However, what constitutes a violation is ultimately determined by the Data Inspection Board, which shall ensure compliance with the rule, and the courts. Provisions on damages and punishments (see Part 16) apply in the event of violations.

Persons who are uncertain of what constitutes a violation or what unstructured material is can instead decide to comply with the provisions of the Personal Data Act. Provided this is done, a violation cannot come into question.

7 Fundamental requirements on the processing of personal data

The controller shall, inter alia, ensure that personal data

- is only processed if it is *lawful*
- is processed in a *proper* manner and in accordance with *good practice*
- is gathered only for specific, explicitly stated and legitimate *purposes*
- is not processed for any purpose that is *incompatible* with that for which the data was gathered
- that is treated is *adequate* and *relevant* to the purpose of the processing
- is only processed if it is *necessary* having regard to the purpose of the processing
- which is processed is *correct* and, if it is necessary, *up-to-date*
- is rectified, blocked or erased, if it is *incorrect or incomplete* having regard to the purpose of the processing
- is not *kept* for a longer period than is necessary.

As regards processing of personal data for historical, statistical or scientific purposes, certain special rules apply. If personal data that is processed for such purposes is also processed later, this shall be considered incompatible with the original purpose for which the data was gathered.

It is also permitted, for such purposes, to save data for a longer period. However, personal data may not be stored in such cases for a longer period than is necessary.

8 Permitted processing of personal data

8.1 General

Personal data may only be processed if the registered person has consented to the processing or the processing is necessary in order

- that a *contract* with the registered person may be performed or measures that the registered person requested may be implemented before a contract is made
- that the controller should be able to satisfy a *legal obligation*
- that *vital interests* of the registered person may be protected
- that a work task of *public interest* may be performed
- that the controller or a third party to whom the personal data is disclosed may be able to perform a work task in conjunction with the exercise of *official authority*
- to satisfy a purpose that concerns a justified interest on the part of the controller or on the part of a third party to whom the personal data is disclosed, provided that this *interest outweighs* the registered person's interest in protection against violation of personal integrity.

The registered person can withdraw his or her consent. When a processing is subject to consent, further personal data may not be processed after the registered person has withdrawn his/her consent.

Even if it would otherwise be permitted without consent having been given, the processing of personal data that is necessary for direct marketing may not take place if the registered person gives written notice to the controller that he/she objects to the processing.

Otherwise, the registered person is not entitled to refuse to acquiesce in the processing of personal data that is permitted under the Personal Data Act.

The list above includes all cases when personal data may be processed.

If sensitive personal data, data concerning violation of laws, etc. or personal identity numbers or temporary personal identity numbers shall be processed, the processing must always be permitted under the provisions applicable to such data (see next part). If personal data is to be transferred to a third coun-

try outside the EU and EEA, processing must also be permissible under the provisions applicable to transfer (see Part 13).

8.2 Processing of sensitive data

It is prohibited to process personal data that discloses race or ethnic origin, political opinions, religious or philosophical convictions and membership of trade unions. It is also prohibited to process personal data relating to health or sexual life.

This prohibition does not apply

- when the registered person has given *explicit consent*
- when the data is *published* by the registered person in a clear manner
- in the case of *necessary processing* to ensure that the controller should be able to fulfil obligations or exercise rights under *employment law*, in order to protect *vital interests* of the registered person or someone else and the registered person cannot provide his/her consent, or to establish, exercise or defend legal claims.
- to processing within *non-profit organisations*
- within *health and hospital care*, if it is necessary for preventive medicine, medical diagnosis, care or treatment, or the administration of health and hospital care.

Sensitive personal data may be processed with the consent of the registered person for research and statistics, provided that the treatment is necessary and provided the public interest in the project manifestly exceeds the risk of improper violation of personal integrity. If the processing has been approved by a research committee, these precautions shall be deemed to be satisfied.

Sensitive personal data may be processed without the consent of the registered person for research provided that the processing has been approved by an ethical review board in accordance with special legislation of ethical consideration of research relating to people.

The Government may issue regulations concerning further exemptions from the prohibition on processing sensitive personal data, if this is necessary having regard to an *important public interest*.

The rules for processing of sensitive personal data apply in addition to the fundamental and general requirements that must be satisfied in all processing of personal data.

8.3 Processing of data concerning violations of laws

It is prohibited for bodies other than authorities to process personal data concerning violations of laws involving crimes, judgments in criminal cases, penal procedural coercive measures, or administrative deprivations of liberty. The prohibition does not apply to decisions in civil disputes, for example cases concerning liability to pay debts.

The Government or the Data Inspection Board may decide on exemptions to the prohibition.

8.4 Processing of personal identity (ID) numbers and temporary personal identity numbers

Data concerning personal identity numbers may be processed without consent only when manifestly justified having regard to the purpose of the processing, the importance of secure identification or some other substantial reason. The same applies to information relating to temporary personal ID numbers, which, in certain cases, are used instead of personal ID numbers.

9 Persons who are registered are entitled to information

9.1 Information which the registered person must always receive

If data concerning a person is gathered from the person him/herself, the controller shall of his/her own volition provide the registered person with information about the processing.

If personal data is gathered from some other source than the registered person, the following applies. The controller shall of his/her own volition provide the registered person with information about the processing when the data is registered.

However, if it is intended to disclose the data to a third party, the information need not be given before the data is disclosed on the first occasion. Information need not be provided at all, if there are regulations concerning the registration or the disclosure of personal data in a statute or some other enactment.

Information never needs to be provided concerning such matters that the registered person is aware of. Nor need information be provided if it proves impossible or would involve disproportionately great effort.

However, if the data is to be used to implement measures that concern the registered person, information shall be provided not later than in conjunction with such use.

The information obligation may be limited by rules concerning secrecy and confidentiality. It may, for example, be mentioned that secrecy within health and hospital care services for data concerning a person's health status also applies in relation to him/herself, having regard to the purpose of the care or treatment, it is of extraordinary importance that the data is not disclosed. A controller that is not a public authority may also apply the provisions of the Secrecy Act to refuse to provide information to the registered person.

The information shall contain information about the identity of the controller and of any agent, the purpose of the processing for which the data is intended and all further information as may be necessary in order to enable the registered person to protect his/her rights in connection with the processing.

Amongst other things, when assessing whether the provision of information would involve disproportionately great effort, the number of registered persons,

the age of the data and the measures that may need to be taken to protect the registered person shall be taken into account.

The duty to inform prescribed by the Personal Data Act applies, in principle, in addition to any duty to provide information prescribed in other legislation, for example within the health and hospital care sector

9.2 Information which the registered person receives after application

The controller is liable to provide, free of charge, notification once per calendar year concerning whether personal data relating to a particular person has been processed or not, provided the person so requests. If such data is processed, written information shall be provided about where the data has been collected, the purpose of the processing and to which recipient or categories of recipients the data is disclosed.

An application for information shall be made in writing to the controller and signed by the applicant personally.

The information shall be provided within one month from when the application was made.

However, if there are special reasons for so doing, the information may be provided not later than four months after the application. Examples of special reasons include the personal data being encrypted, limited search possibilities, or that considerable quantities of data that are located in several different registers or databases are involved.

Information need not be provided about personal data in running text that had not yet been given its final form when the application was submitted or which takes the form of working notes or the like. Notwithstanding this, information shall be provided to the applicant if the data has been disclosed to a third party or if the data is only processed for historical, statistical or scientific purposes or, as regards running text that has not been given its final form, if the data has been processed for a longer period than one year.

As with information that must be provided voluntarily (see Part 9.1), the rules concerning secrecy and confidentiality also apply in this case instead of the duty to provide information.

The information must be comprehensible for the registered person. As regards information concerning the source of the information, the controller need only provide the information that is available to him/her. Thus the controller does not need to keep track of where data has been collected, but if he/she knows this when the registered person requests information it must be provided. Agency decisions on information may be appealed against to a court.

10 Certain decisions through data processing

In the case of automated decisions, there is a special right in certain cases to request that such a decision be reviewed manually, i.e. by a human being.

If a decision that has legal consequences for a natural person or has other manifest effects for the person, is based solely upon data processing of personal data that is intended to assess characteristics of the person affected, the person is entitled on request to have the decision by a person.

Anybody who has been subject to such decision is thus entitled, upon request, to obtain information from the controller concerning what has governed the data processing that generated the decision. Appeal may be made to a court against agency decisions on such information.

11 Rectification

The controller is liable, upon request, by the registered person, to correct, block, restrict or erase as soon as practicable such personal data as has not been processed in accordance with the Personal Data Act or regulations issued under the Act. For example, this may relate to incorrect data or data that has not yet been processed because they are sensitive.

The controller shall also advise a third party to whom the data has been disclosed about the measure if the registered person so requests or if rather substantial damage or inconvenience for the registered person may be avoided by a notification. However, such notification need not be given if it proves impossible or would involve disproportionate effort.

The controller must on his/her own initiative be active in ensuring that the personal data processed is correct. However, the registered person may also demand that the data is rectified.

If disagreement arises between the controller and the registered person about whether data should be corrected or not, the registered person may report the matter to the Data Inspection Board. Appeal may also be made to a court against agency decisions on rectification.

It is the person who must perform the rectification, i.e. the controller, who decides which of the alternative methods of rectification, blocking and erasure shall be selected in various selections.

12 Security when processing data

A person working with personal data may only process the data in accordance with instructions from the controller. If a statute or other enactment contains special provisions concerning the processing of personal data in public operations on such matters, these provisions shall apply.

The controller is liable to implement technical and organizational measures to protect the personal data. The measures shall attain a suitable level of security.

When the controller engages an assistant to conduct the processing of personal data, there shall be a written contract that specifically regulates the security aspects. The controller shall also be responsible to ensure that the assistant actually implements the necessary security measures.

If someone who works for the controller discloses personal data in contravention of that provided by the Personal Data Act, it is the controller who bears the legal responsibility in relation to the registered person.

The Data Inspection Board should, to a reasonable extent, provide advice on security matters. Inadequacies in security are unacceptable. Consequently, the Data Inspection Board has clear powers specifically relating to security. The Personal Data Act contains an explicit provision that the supervisory authority may issue decisions on security measures in individual cases. The controller receives by such decision notifications of what measures he/she must implement to satisfy the security requirements.

It is the controller who is responsible in relation to the registered person as regards the processing, even if an assistant has been engaged.

13 Transfer of personal data to a third country

In principle, it is forbidden to transfer personal data that is being processed to a third country (a country outside the EU and EEA) that does not have an adequate level of protection for personal data.

It has been established by guideline cases from the European Court of Justice and the Swedish Supreme Court that publication of personal data on Internet does not normally entail a transfer of information to all countries that have access to the Internet. This means that it is not necessary to comply with the provisions on transfer of personal data to a third country when personal data is published on the Internet via a computer within the EU and EEA. However, when publishing data, the other requirements of the Personal Data Act must be complied with.

The issue of whether the level of protection in a country is adequate shall be assessed taking into account all the circumstances related to the transfer. Particular importance shall be attached to the nature of the data, the purpose of the processing, the length of time the processing will take, the country of origin, the final country requesting the data and the rules applicable for processing in the third country. The issue of whether the level of protection in a particular country is adequate may thus be assessed in various ways depending upon the circumstances in the individual case. It is conceivable that a country has an adequate level of protection in certain fields but not in others

Even if the third country in question does not have an adequate level of protection, it is allowed to transfer personal data to such country if the registered person has given his/her consent to the transfer or when the transfer is necessary in order that

- a *contract* between the registered person and the controller may be performed or measures that the registered person requested may be taken before a contract is made
- a *contract* between the controller and a third party that is in the interests of the registered person may be made or performed
- *legal claims* should be established, exercised or defended
- *vital interests* of the registered person may be protected.

It is also permitted to transfer personal data for use solely in a state that has acceded to the Council of Europe Convention of 28 January 1981 on the protection of individuals in automatic data processing.

The Data Inspection Board can provide details of these countries.

As regards matters of computer processing, the Government may also issue regulations concerning exemptions for transfer of personal data to certain states. The Government may do this if it is shown that a third country has a sufficient level of protection for personal data to be transferred.

The Government may also, as regards matters of computer processing of personal data, issue regulations permitting transfer of personal data to a third country, if the transfer is regulated by an agreement that provides sufficient guarantees of the rights of the registered persons.

Furthermore, the Government or the Data Inspection Board, may, as regards matters of computer processing, issue regulations concerning exemptions, provided it is necessary having regard to vital public interests or if there are sufficient safeguards to protect the rights of the registered persons.

14 Notification of processing of personal data

The former licence and permit system has been abolished. The operations of the Data Inspection Board have instead been concentrated on providing advice about the substantive rules and the supervision of compliance with the rules.

According to the Personal Data Act, there is a primary obligation to notify all data processing to the supervisory authority, which must maintain a register of the notifications. However, if the controller has appointed a data representative – and given notice of this to the Data Inspection Board – notifications concerning processing need not be given. The Government or the Data Inspection Board may issue regulations concerning exemptions from the duty to give notice for such kinds of processing as are not likely to result in an improper violation of personal integrity.

The Government may issue regulations that particularly sensitive processing must be notified to the supervisory authority for prior examination three weeks in advance. This applies even if a data representative has been appointed.

The controller is under a duty to provide to anyone who so requests, expeditiously and in a suitable manner, information concerning computer and other processing of personal data as has not been notified to the Data Board. Appeal may be made to a court against agency decisions on such information.

15 Supervision

The Data Inspection Board is the supervisory authority under the Personal Data Act and has, in such capacity, the right of access to the personal data processed, information about and the documentation of processing, and is also empowered to enter premises connected with the processing.

If the Data Inspection Board cannot obtain sufficient information to establish that the processing is lawful, it may prohibit the controller, on pain of a fine, from processing personal data in any other manner than by storing it. This also applies, if following an unlawful processing, it is found that it is not possible to effect rectification in any other way or if the matter is urgent.

The Data Inspection Board may apply to the County Administrative Court of the erasure of data that has been processed in an unlawful manner. This power may only be utilised when it is not possible to combine, by other measures, the processing of the data with the applicable rules. A decision on erasure may not be issued if it would be unreasonable.

Appeal may be made against a decision by the Data Inspection Board to a general administrative court, i.e. in the first instance the County Administrative Court. The Data Inspection Board may decide that a decision should apply even if it is appealed against.

16 Damages and criminal penalties

The controller shall compensate the registered person for damage and violation of personal integrity caused by the processing of personal data in contravention of the Act. However, if the controller shows that the error was not caused by him or her, the obligation to pay compensation may, to the extent reasonable, be reduced or lapse completely.

A person who has intentionally or by gross negligence disclosed untrue data in information or notifications under the Act, or who in contravention of the provisions of the processes sensitive personal data or data concerning offences, etc. or transfers personal data to a third country or neglects to give notice concerning the processing to the supervisory authority may be sentenced to a fine or imprisonment of at most six months. If the offence is grave, the penalty is at most two years' imprisonment. A sentence shall not be imposed in petty cases. The same applies to a person who, when processing personal data in unstructured material, violates the personal integrity of the registered person by processing sensitive personal data or information on violations of the law, etc. or by transferring personal data to a third country which does not have an adequate level of protection of personal data.

Ministry of Justice, Sweden

Tryck: Edita Stockholm 2006. Omslag: Rolf Hernegran. Upplaga: 1000 ex.