

# Trends in Data Protection Law

Sören Öman

<b>1</b>	<b>Introduction .....</b>	<b>210</b>
<b>2</b>	<b>Amendments 2007 to the 1998 Swedish Personal Data Act .....</b>	<b>212</b>
<b>3</b>	<b>Swedish Special Data Protection Laws in the Public Sector .....</b>	<b>221</b>

## 1 Introduction

The first national legislation aimed at protecting the informational privacy of individuals when their personal data are processed in computers saw the light of day in Sweden in 1973. The Swedish 1973 Data Act only covered processing of personal data in traditional, computerised registers. The act did not contain many material provisions on when and how the data should be processed, or general data protection principles. Instead, the act required for each computerised personal data register a prior permit from a new data protection authority – the Data Inspection Board. When a permit was given, the Board issued tailor-made conditions for that register.

Soon, the general 1973 Data Act was supplemented by a number of special data protection laws covering particular computerised personal data registers held by authorities. Those special data protection laws contained tailor-made provisions for each register.

Sweden has acceded to the 1981 Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data, but the accession did not result in any major amendments to the 1973 Data Act.

By the end of the 1980s, although the 1973 Data Act had been amended several times over the years, the 1973 Data Act was hopelessly out-dated. In 1989 a Commission on Data Protection was set up by the Swedish Government to make a total revision of the 1973 Data Act. This coincided with the European Commission's first proposal for an EC Directive on data protection (OJ No 277, 5.11.1990, p. 3). The Swedish Commission worked for about four years and submitted its final report in 1993. The Commission recommended (SOU 1993:10) the enactment of a new Data Protection Act based, by and large, on the then current second proposal from the European Commission for an EC Directive (OJ C 311, 27.11.1992, p. 30). Since Sweden was not even a member of the EC at that time – the EEA Agreement came into force on 1 January 1994 and Sweden became a member of the EU one year later – several authorities and organisations that were consulted were negative to a premature implementation, and the Commission's recommendation was not followed.

In 1995, after some five years of discussion, the European Union adopted a directive on data protection (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data), and a new Swedish Committee was, even prior to the formal approval by the EU of the directive, entrusted with making recommendations on the implementation of the directive and a new total revision of the 1973 Data Act. The Committee presented in 1997 a report on the implementation (SOU 1997:39) containing a proposal for a new Personal Data Act.

The Committee noted that the directive, and the data protection principles contained in other international instruments, necessitated the regulation of all handling of personal data, from collection to deletion. Consequently, the Committee had to base its proposal for a new Personal Data Act on a model for regulating all handling of personal data, and the proposed act was more or less a transcript of the directive. The Committee, however, would have preferred a model that for common, everyday, processing not connected to large databases

did not regulate all handling of personal data but instead only prevented abuse (misuse) of such data. The Swedish government shared the views of the Committee and said that its intention was to influence the European Union to abandon the present all-encompassing regulatory model with rules covering all steps in the handling of personal data (Government Bill 1997/98:44 p. 36–37).

The new Personal Data Act came into force in October 1998, and immediately triggered a media storm of seldom seen proportions as well as uproar among tens of thousands of Internet users under the slogan “Don’t touch my Internet” soon followed by petitions from all political parties in the Swedish Parliament for amendments to the act. The main concern was the effect of the new act on the publication of personal data on the Internet. The Parliament responded with a three-tier action plan (Report KU 1998/99:15). In the short-term perspective amendments should be made to the provisions in the act on transfer of personal data in order to facilitate the publication of personal data on the Internet. In the mid-term perspective a review of the act should be made in order to achieve, as far as possible within the limits of the directive, a regulation that is based on preventing abuse of personal data rather than on regulating every step of the handling of such data. In the long-term perspective amendments to the directive in that direction should be made and the government should act decisively within the European Union to achieve that. Amendments to the provisions in the act on transfer of personal data entered into force on 1 January 2000 (SFS [the Swedish Official Journal] 1999:1210, Government Bill 1999/2000:11).

As regards the long-term strategy of having the directive amended, the Swedish Ministry of Justice has presented a draft proposal for amendments to the directive exempting from the regular provision in the directive the processing of personal data in non-structured material, such as word processing and publication of text on the Internet. The main argument for the new approach is that since computers today have become a tool for information-handling used every day by everybody everywhere for everything it is not reasonable to apply the traditional, bureaucratic data protection principles which require the person handling the personal data, writing an e-mail, for example, to apply several rules before concluding if and under what circumstances the processing can be carried out.

Sweden has gained support from several Member States in the European Union for the idea of having the directive amended, although not to the extent that Sweden is prepared to go. Sweden has also, with some success, tried to influence the Council of Europe to review the data protection principles in the Convention 108 for the protection of individuals with regard to automatic processing of personal data.

As regards the mid-term strategy of trying to amend the Swedish 1998 Personal Data Act along the lines of an abuse centred model within the boundaries of the directive, I was in 2002 appointed special investigator commissioned to carry out the review of the act. At the beginning of 2004, I presented a report containing draft amendments to the act along the lines of an abuse centred model, see SOU 2004:6. The proposed amendments were carried through and came into force 1 January 2007.

It has long been a specific feature of Swedish data protection law that it comprises a system with innumerable acts with special data protection provisions covering different sectors of the public administration or a particular, big, computerised personal data file held by an authority. This system has not been abandoned with the introduction of the 1998 Personal Data Act. Instead, most existing special data protection acts were adapted to the new Personal Data Act or replaced by new acts. In fact, after the entry into force of the Personal Data Act several special data protection acts covering important areas of the public administration that were not previously covered by any special data protection regime have been adopted. Even today, there are several proposals for amended or brand new special data protection acts pending or being prepared.

The Swedish implementation of the directive has been presented in detail elsewhere. It has even been the subject of a doctoral thesis in history (Lars Ilshammar, *Offentlighetens nya rum, Teknik och politik i Sverige 1969–1999*, Örebro 2002) and there are accounts in English as well (Peter Seipel in Peter Blume [ed.], *Nordic Data Protection*, Copenhagen 2001, and Sören Öman in Wolfgang Kilian [ed.], *EC Data Protection Directive – Interpretation/Application/Transposition – Working Conference*, Darmstadt 1997). The arguments for a shift from the traditional regulation of all handling of personal data to a new abuse centred regulatory model have also been presented in English elsewhere (Sören Öman, *Protection of Personal Data – But How?* in Law and Information Technology. Swedish Views SOU 2002:112 pp. 177–184). I will therefore not here go into further detail regarding the implementation or the arguments for a new approach. Instead, I will present, firstly, the 2007 amendments to the 1998 Personal Data Act and, secondly, the Swedish system with special data protection laws for processing of personal data in the public sector.

## **2 Amendments 2007 to the 1998 Swedish Personal Data Act**

The main objective of my review of the 1998 Personal Data Act was to examine whether it is possible, despite the directive, to replace the current regulations on the handling of personal data with regulations against the misuse of personal data. In connection with the implementation in 1998 of the directive the government and Parliament made the assessment that this was not possible since the provisions in the directive on the handling of personal data had to be implemented.

It is obvious that the provisions in the directive on the handling of personal data (when is it legal to process personal data, what information must be provided to the data subject etc.) must be implemented. Those provisions are in fact, by and large, adequate, reasonable and necessary when it comes to the processing of personal data in traditional databases and personal data files, and the application of those provisions to such processing is, more or less, accepted by the general public and controllers in Sweden. What has been heavily criticised in Sweden is instead the application of those principles to the everyday processing of personal data in unstructured material, such as running text (free-format text) and sound and image data, especially in connection with the publication of such data on the Internet. The strategy of my review was therefore

to leave the provisions in the Personal Data Act that implement the provisions in the directive untouched but to try to make full use of the possibilities in the directive to deviate from those provisions as regards processing of personal data in unstructured material.

My conclusion was that it is in fact possible to deviate from the provisions in the directive on handling of personal data as regards such processing of personal data in unstructured material as can not be construed as an abuse of the data. A unanimous expert group supported that conclusion, and my consultations with representatives from all political parties represented in Parliament did not reveal any objections.

There are in the directive several possibilities for exemptions, deviations and derogations. Some possibilities had already been used to full extent in the Personal Data Act. That was the case as regards the possibilities to exempt from the act purely personal activities (article 3.2 second indent in the directive and section 6 in the act) and processing carried out solely for journalistic purposes or the purpose of artistic or literary expression (article 9 in the directive and section 7 in the act). Other possibilities had not yet been used to their full potential.

According to article 13 in the directive it is possible to restrict the application of several articles in the directive provided that such a restriction constitutes a necessary measure to safeguard the protection of the rights and freedoms of others. The question for me was whether the handling of running text and other unstructured material, containing personal data, without being restricted by the provisions on the handling of personal data referred to in article 13.1 could be regarded as such a right or freedom. My conclusion was that it can. Reference was here made to the Swedish constitution and to article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, which guarantees the right to freedom of expression including freedom to hold opinions and to receive and impart information. Article 13 in the directive only allows for restrictions that are “necessary” to safeguard rights and freedoms. This necessity requirement was met by exempting from the provisions in the directive only such handling of personal data in unstructured material as can not be construed as an abuse of the data.

Article 13 in the directive allows for (necessary) exemptions from articles 6.1, 10, 11.1, 12 and 21. Article 6.1 contains most of the traditional data protection principles, the principles of fairness and lawfulness, the purpose specification and limitation principle, the data quality principle and the collection limitation principle. Articles 10–12 concern information to be provided to the data subject on the controller’s own initiative in connection with the collection of the personal data or on the data subject’s request (subject access), and article 21 concerns the provision of general information on processing operations being carried out.

Article 13 in the directive does not, however, allow for exemptions from the provisions in article 7 on the requirement for a legal ground for the processing of personal data. It was therefore necessary to find in article 7 a legal ground for the processing of personal data in unstructured material. A legal ground for processing is according to article 7 f that the processing is necessary for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests of the data subject. If the handling of

unstructured material, including personal data, can, as explained above, be seen as an enjoyment of a right or freedom, then the, legitimate and fundamental, interests of the controller clearly outweigh those of the data subject, provided of course that the handling of the personal data does not amount to an abuse of the data. My conclusion was therefore that it is possible to base a provision in the Swedish act allowing such handling on article 7 f in the directive.

According to article 14 a in the directive the data subject shall in the case referred to in article 7 f be granted the right to object at any time on compelling legitimate grounds relating to his or her particular situation to the processing of data relating to him or her, “save where otherwise provided by national legislation”. The possibility for exemption in the cited passage had in Sweden already been used to full extent. There was namely already an explicit provision in the act to the effect that the data subject has no right to object to such processing as is allowed according to the act, except processing for direct marketing purposes.

Furthermore, article 13 in the directive does not allow for exemptions from the provisions in article 8. In article 8.1 there is a ban on the processing of special categories of data, such as sensitive personal data for instance revealing political opinions or concerning health. It is, however, according to article 8.4, allowed to make exemptions from that ban for reasons of substantial public interest, if suitable safeguards are provided. Since the handling of unstructured material, including sensitive personal data, can, as explained above, be seen as an enjoyment of a right or freedom, it is of course a “substantial public interest” that that right can be protected. And the requirement for “suitable safeguards” can be met by exempting only such handling of sensitive personal data in unstructured material as can not be construed as an abuse of the data. My conclusion was that it is possible to base an exemption from article 8.1 for the handling of sensitive personal data in unstructured material on article 8.4.

The principle rule in article 8.5 in the directive is that personal data relating to offences, criminal convictions or security measures may only be processed under the control of official authority. There is, however, a possibility to make derogations from that rule if there are national provisions providing suitable specific safeguards. It was therefore in my opinion possible to allow in general the handling of unstructured material, including personal data relating to offences, criminal convictions or security measures, provided that the handling does not constitute an abuse of the personal data. The latter rule – the prohibition on abusive handling – can be seen as a “suitable specific safeguard”.

There is also no possibility to use article 13 in the directive to deviate from the ban in article 25.1 on transfer of personal data to third countries outside the EU- and EEA-area that do not ensure an adequate level of protection. It is, however, according to article 26.1 d possible to transfer personal data to such third countries if the transfer is necessary on important public interest grounds. With corresponding reasoning as that explained above in connection with article 8.4 it was, in my opinion, possible to introduce in the Swedish act a provision making the handling of unstructured material, including the transfer to third countries of the personal data contained in the material, legal provided that the handling does not constitute an abuse of the personal data.

As regards the obligation according to article 18.1 in the directive to notify the supervisory authority of processing operations, there is according to article 18.2 first indent a possibility to exempt from the obligation to notify categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects. This possibility had already been used in Sweden to exempt from the obligation to notify the processing of personal data in running text, see section 4 in the Personal Data Ordinance, SFS 1998:1191. My conclusion was that it is possible to use article 18.2 first indent to exempt also all other processing of personal data in unstructured material from the obligation to notify.

This renewed analysis of the possibilities in the directive for exemptions, deviations and derogations led me to propose a new provision in the Personal Data Act to the effect that processing of personal data in unstructured material is not subject to most of the normal rules on processing of personal data in the act.

One difficulty was to define the processing of personal data in unstructured material that is to be exempted. As soon as something has been put into a computer in binary format it has in some way been structured. The technological developments had made it easier to both automatically structure everything – i.e. through automatically applied indexing of text – and retrieve data in unstructured material, thereby structuring the data.

The starting point for me was that *material – a set of data – structured with reference to personal data* shall not fall under the exemption. Material is structured with reference to personal data if personal data in the material has in some way been marked as personal data. This is the case, for example, when there is a field in a database where the name of a natural person – the client, a contact person, the person handling a particular case etc. – is to be entered. If a material has been structured only in general, there is no structure with reference to personal data. When every word on a hard disc has been indexed, there is no structure with reference to personal data but only a general structure, provided that no personal data have been in some way marked as such.

An additional requirement for the material structured with reference to personal data not to fall under the exemption is that the material has been structured in order to *significantly* facilitate searches for or compilations of personal data specifically. The significantly criterion is used to exempt everyday processing operations in two cases.

Firstly, the criterion is used to exempt what I call a banal structure with reference to personal data. This is the case when personal data have been structured only in the meaning that they have been entered in a particular order, i.e. an alphabetical list of persons on a web page or in a word processor document. This exemption is of course not applicable if the list has been generated using a database.

Secondly, the criterion is used to exempt what I call commonplace use of everyday functions where the structure with reference to personal data is not particularly elaborate. Here I only had two examples. The first one is the use of a computer's file system. If you use the names of individuals to name the files and catalogues in your computer, you have created a structure with reference to personal data, but such commonplace practices should nevertheless be exempted. The second example is the normal use of e-mail software, or other

software for communication. Such software automatically puts personal data in a particular field, describing the recipient or sender, to be able to perform the communication, thereby creating a structure with reference to personal data. The normal use of software for communication should however be exempted. The exemption is of course not applicable if the files or e-mails are included in a document handling system.

In one set of data is included all data that can be attributed to the personal data that has been structured. This means that also personal data that has not been structured can form part of a set of data, personal data contained in scanned documents attributable to the author's name in a document handling system, for example.

The definition discussed briefly above was of course difficult to include in detail in a provision in the Personal Data Act. The Swedish legislative tradition is however to have a concise provision in the act itself combined with explanations in the legislative comments, which are subsequently consulted for guidance by the judiciary, legal scholars and advisors and, sometimes, even the general public. According to this tradition I proposed a new provision in the Personal Data Act. The proposal was accepted with only minor adjustments and a new section (5 a) was introduced in the Personal Data Act as of 1 January 2007 (SFS 2006:398):

“It is not necessary to apply the provisions in sections 9, 10, 13–19, 21–26, 28, 33, 34 and 42 to processing of personal data that do not form part of and are not intended to form part of a set of data that has been structured in order to significantly facilitate searches for or compilations of personal data specifically.

Such processing as is referred to in the first paragraph may not be carried out if it entails a violation of the personal integrity of the registered person.”

As can be seen, an exemption is made from several of the provisions in the act. The exempted provisions in the act correspond to the following provisions in the directive:

- a) Principles relating to data quality – Article 6;
- b) Criteria for making data processing legal – Article 7;
- c) Processing of special categories of (sensitive) data – Article 8.1;
- d) Processing of data relating to offences, criminal convictions or security measures – Article 8.5;
- e) Use of personal identification numbers – Article 8.7;
- f) Information in cases of collection of data from the data subject and information where the data have not been obtained from the data subject – Articles 10 and 11;
- g) Subject access – Article 12 a;



- h) Rectification, erasure or blocking of data – Articles 12 b and c;
- i) Transfers of personal data to third countries – Article 25.1;
- j) Publicizing of processing operations – Article 21.3.

One may note in particular that an exemption is made from the right to subject access, i.e. the right for the data subject to have on request an extract of the personal data processed, section 26 in the act and article 12 a in the directive. I did not propose that exemption since I considered that right to be of fundamental importance for the data subject. It can of course be difficult for the controller to locate on request all data pertaining to a particular data subject contained in unstructured material, or if the controller has a very large number of registers or material in many different places, in hundreds of computers, for instance. Therefore I proposed amendments to the provision on subject access to make it less onerous on the controller in this case. The government, however, took the position that also the provision on subject access should be exempted and that it was not necessary to make that provision less onerous (Government Bill 2005/06:173 p. 40–41 and 49–50).

The second paragraph in the new section in the act contains a provision on abuse of personal data, i.e. processing that entails a violation of the personal integrity of the data subject. It is a general provision that has to be interpreted by the courts and the Swedish Data Inspection Board supervising the application of the act.

Apart from the Personal Data Act there are several other provisions in Swedish law that are general and not limited to such processing as is covered by the Personal Data Act which protect the personal integrity of individuals, inter alia provisions on secrecy and slander. In many instances those provisions will give an adequate protection for the personal integrity of individuals also in connection with such processing of personal data as is covered by the Personal Data Act and the directive. As regards the interpretation of the proposed provision in the Personal Data Act on abuse of personal data I provided a list of some simple rules of conduct when processing personal data in unstructured material:

- Do not process personal data for improper purposes, such as persecuting or disgracing an individual.
- Do not collect a large amount of information about one individual without acceptable reasons.
- Rectify personal data that turn out to be incorrect or misleading.
- Do not slander or insult anyone.

- Do not violate an obligation to keep information secret.

If a controller adheres to the exempted provisions in the Personal Data Act when processing personal data in unstructured material, the processing can obviously not constitute a violation of the personal integrity. This means that a controller that has doubts whether a certain processing operation is exempted or could constitute a violation of the personal integrity can choose to follow the “normal” rules for that processing operation.

The government repeated my list of simple rules in the legislative comments in the Government Bill but stressed that it was ultimately up to the courts and the Swedish Data Inspection Board to weigh in each case the intrusion of the personal integrity against other interests (Government Bill 2005/06:173 p. 29).

The Data Inspection Board shall supervise the application of the new provision and a violation of that provision can constitute grounds for damages to the affected data subject according to the normal provisions on damages in the Personal Data Act. A violation of the new provision can in some instances also be an indictable offence.

One clear legislative trend has thus been to make it easier for controllers to process personal data in unstructured material. The practical impact for controllers of the amendments depends much on how the Data Inspection Board and the courts choose to interpret the provision on abuse of personal data, which is formulated in a general way. Cases decided by courts are still rare and I know of only a couple of court cases regarding camera surveillance. The Data Inspection Board has, however, published decisions in several cases but they seem more or less restricted to two distinct areas: publication on the Internet and camera surveillance. It should also be noted that the definition of the exempted processing operations does not seem to have caused any difficulties worth mentioning.

As regards publication on the Internet the Data Inspection Board has found that the following cases constituted a violation of the personal integrity:

- Publication by a municipal school of the names of pupils being suspended from the school;
- Publication by a blogger of purely private personal information of a sensitive nature (alleged sexual abuse against a child etc.) in a custody case;
- Publication by a county council of the name of a person lodging a complaint against the council and of personal data regarding a patient incarcerated in a psychiatric clinic.

In another case the Data Inspection Board found that the publication on the Internet by a private corporation of precedence judgements from the Swedish National Labour Court did not constitute a violation of the personal integrity.

In my opinion those decisions published by the Data Inspection Board were all clear cases. It seems that the Board has been reluctant to become a general sentinel of publications on the Internet and restricted its efforts to clearly abusive publications.

In some cases where a claim for damages is raised against the state the Swedish Chancellor of Justice has to interpret the Personal Data Act. The Chancellor of Justice has in one case found that the publication by a university of a job application constituted a violation of the personal integrity of the applicant, who received general damages in the amount of SEK 3,000 (approx. EUR 300). This may seem as a considerably more extensive application of the provision on abuse of personal data than that applied so far by the Data Inspection Board. A closer examination of the case reveals, however, that the open publication on the Internet of the job application was unintentional. The processing could therefore be seen as a violation of (not the provision on abuse of personal data but rather) the provisions on the security of the processing (articles 16 and 17 in the directive), which are not exempted.

The Chancellor of Justice has found that the publication on the Internet by the police of a surveillance video of a robbery, which contained identifiable images of one victim of the robbery, for crime fighting purposes did not constitute a violation of the personal integrity.

When it comes to social media on the Internet – Facebook, My Space, blogs, Twitter etc. – the databases behind the social media sites usually contain structured personal data and the processing of such data in those databases is consequently not exempted. The content on social media sites is, however, to a large extent generated by the users and not *per se* structured. There are often three different categories of actors providing content: (i) the corporation behind the social media site; (ii) the user instituting a page on the media site (a page on Facebook, a blog on a blog site etc.); (iii) the user providing content on a page by writing comments or uploading material.

The Data Inspection Board has found that the corporation behind a social media site is the controller for all processing of personal data in the databases behind the site, also the content provided by (or rather, collected from) users, and that the processing is not exempted. Furthermore, the Data Inspection Board has found that (also) the user instituting a page on the social media site is the controller not only for his or her own processing of personal data but also for the processing of personal data done by other users when they provide content on that page. As regards Twitter accounts the Board found that the account holder is the controller for the processing of personal data only in his or her own messages and not for the processing of personal data in messages from other users sent through the account, since there is on Twitter no constant page instituted where the account holder can remove or edit messages from other users. The Data Inspection Board did not rule out that (also) users just providing content could be considered as controllers as regards the processing of personal data in the content provided.

The Data Inspection Board found that the processing for which a user instituting a page is the controller is exempted since that user is not provided with the means to structure the personal data on the page in order to significantly facilitate searches for or compilations of personal data specifically.

The legal situation as regards the responsibility for the processing of personal data in content on social media sites is, provided that the assessments made by the Data Inspection Board are correct, complicated. It may seem surprising that the Board chose to complicate the legal situation by considering also users as

controllers, subject almost exclusively to the provision on abuse of personal data, when there already is someone – the corporation behind the social media site – with full responsibility according to the Personal Data Act for the very same processing of personal data. It should, however, be noted that the corporations behind social media sites are often established outside EU and therefore out of reach for the Data inspection Board.

Many decisions from the Data Inspection Board have concerned camera surveillance, i.e. surveillance through a fixed, not handheld, electronic camera. Traditionally such camera surveillance has been regulated by special legislation and not by the general data protection legislation. Today camera surveillance is regulated by the 1998 Act on General Camera Surveillance (and, as regards secret camera surveillance done by certain authorities, another act). That act is supplemented by the provisions in the Data Protection Act. The problem is that the 1998 act is outdated and has been under review since 2001. A second proposal for a new act was presented by an inquiry in 2009 (SOU 2009:87). The 1998 act requires a prior permit or in some cases only prior notification for installing a camera able to capture persons in a place to which the general public has access, such as a store or the entrance to an office. For camera surveillance of other places the 1998 act contains only a couple of basic provisions and the provisions in the Personal Data Act are thus of more importance in those cases. According to the 2009 proposal the new act shall contain the material provisions on camera surveillance and exclude the application of the Personal Data Act.

The decisions from the Data Inspection Board are concentrated on three areas: Camera surveillance (i) in apartment buildings; (ii) in schools; (iii) in the workplace.

As regards camera surveillance in apartment buildings the Data Inspection Board has inspired several landlord organisations to draw up a joint code of conduct including provisions on camera surveillance on which the Board issued a favourable opinion in 2010. The Data Inspection Board has taken the position that camera surveillance of areas which the tenants have to pass to get to their apartments, i.e. entrances, corridors, etc., constitutes a violation of the personal integrity. The Board has on the other hand accepted camera surveillance of other areas such as laundry-rooms, refuse collection rooms, cellars and attics, at least if some kind of problem has been experienced in those areas and other measures are not practical. Also electronic peep-holes in the apartment doors have been accepted.

The Data Inspection Board has in several decisions taken the position that camera surveillance inside schools during school hours constitutes a violation of the personal integrity. I know of only one case where the Board has accepted such camera surveillance. That case concerned camera surveillance, for the purpose of preventing theft, of a secluded space with lockers for school computers which the students had to visit only when depositing or retrieving a computer.

A couple of cases have concerned camera surveillance in the workplace. The Data Inspection Board has taken the position that using camera surveillance to monitor the work performance of individuals normally constitutes a violation of the personal integrity. In some cases the Board also found that the information provided to the employees was insufficient.

A comparison between the cases where the Data Inspection Board has found a violation of the personal integrity through publication on the Internet and the cases where the Board has come to the same conclusion regarding camera surveillance seems to indicate that the threshold for something to be a violation of the personal integrity is considerably lower in the latter cases according to the Board. This shows in my opinion that a general provision aimed at preventing only misuse of personal data, i.e. just severe cases, is not suitable for handling the specific type of processing that camera surveillance constitutes. There is a need for more and clearer provisions for camera surveillance to provide enough guidance for controllers as well as an acceptable level of surveillance in the society.

The cases concerning open publication on the Internet have a clear connection to the fundamental right of freedom of expression, which is lacking in the cases concerning camera surveillance. This might explain why the threshold for something to be a violation of the personal integrity seems to be higher in the former case. It might also explain why the Chancellor of Justice applied a seemingly low threshold when he found the publication on the Internet by an authority of a job application containing only harmless personal data to be a violation of the personal integrity. The fundamental right of freedom of expression is a right for individuals that is to be respected by authorities and other parts of the state, not a right for authorities.

### **3 Swedish Special Data Protection Laws in the Public Sector**

If another act or an ordinance contains provisions that deviate from the Personal Data Act, those provisions shall apply according to section 2 in the Personal Data Act. The Personal Data Act is thus subordinate to other legislation, which takes precedence over the general provisions in that act. In Sweden, acts are decided by parliament and ordinances by the government.

There are several acts and ordinances containing tailor-made data protection provisions for specific sectors of the public administration or a particular personal data file held by an authority. There is, for example, special data protection legislation covering the processing of personal data

- in the health sector (SFS 2008:355),
- by the police (Police Data Act, SFS 2010:361),
- on persons liable for military service by the armed forces (SFS 1998:938),
- by the tax and customs authorities when conducting criminal investigations or preventing crime (SFS 1999:90 and 2001:85),
- for the production of Sweden's official statistics (SFS 2001:99),
- by the tax authorities for taxation purposes (SFS 2001:181) and for the purpose of keeping the national register of persons (SFS 2001:182),
- for electoral purposes (SFS 2001:183),
- by the Swedish enforcement service (SFS 2001:184),
- by customs authorities (SFS 2001:185),
- by the social services (SFS 2001:454),
- by the prison and probation administration (SFS 2001:617),

by the courts (SFS 2001:639–642),  
by the armed forces and the national defence radio establishment (SFS 2007:258 and 2007:259),  
by the labour market authorities (SFS 2002:546), and  
by the social security authorities (SFS 2003:763).

The following are examples of special data protection legislation covering particular personal data files:

The national register of personal addresses (SFS 1998:527)  
The register of criminal records and suspicions of criminal acts (SFS 1998:620 and 1998:621)  
The register for forensic psychiatry (SFS 1999:353)  
The register of property damaged in a war (SFS 1999:889)  
The land register (SFS 2000:224)  
The register of dogs and their owners (SFS 2007:1150)  
The register concerning insider trading (SFS 2000:1087)  
The register of vehicles (SFS 2001:558)

The explicit ambition has been to have a special data protection regime decided by parliament (i.e. in an act) for every personal data file held by authorities covering a large number of persons and including sensitive material (see Government Bills 1990/91:60 p. 50 and 1997/98:44 p. 41 and Reports by the parliamentary committee on constitutional matters 1990/91:11 p. 11 and 1997/98:18 p. 43). The general rule is that the special data protection legislation should complement the generally applicable Personal Data Act and contain only the necessary deviations from the provisions in that act. The special data protection acts, decided by parliament and containing only the basic data protection provisions, are often supplemented by special data protection ordinances, decided by the government, and regulations, decided by an authority, containing more precise provisions on the exact content of the personal data file, for example, and, to the extent allowed by the act, precise deviations from the act regarding external electronic access to the personal data file, for example.

This legislative approach has led to a complex web of data protection provisions in, at least, four layers: The general Personal Data Act, the special data protection act decided by parliament, the special data protection ordinance decided by the government and the special data protection regulations issued by some authority. In addition, the authorities have to keep track of several hundreds of provisions on secrecy in the Secrecy Act (SFS 2009:400), also protecting the privacy of individuals, and innumerable provisions on obligations to provide information scattered throughout the whole body of Swedish legislation. The relationship and hierarchy between different provisions can sometimes be difficult to determine.

The complexity and diversity has in later years been criticised by several state inquiries and the need for a more unified approach has been stressed, see SOU 2005:117, SOU 2007:45 and SOU 2010:4, for example. Also a state inquiry with members from all political parties represented in parliament has unanimously

expressed concerns, see SOU 2007:22. As yet, no official initiative has been taken by the government.

In connection with the entry into force of the 1998 Personal Data Act the then existent special data protection legislation was reviewed and amended to adjust to the new act and legislation covering areas not previously covered was enacted. It later turned out that many of those acts and ordinances lacked long term stamina. In several cases a review of the legislation was initiated only a couple of years after the enactment. This was the case as regards the police sector, the health sector and the social services sector. Several acts covering new areas are also being prepared. A large part of the administrative resources available for lawmaking, especially lawmaking not required to implement EU law, has been spent on preparing and updating special data protection legislation.

One trend for the state administration has been to have only one authority for one sector instead of the previous system with one central authority with several subordinate regional and local authorities. Today, the police, the courts and the general regional state administration are organised according to the latter model whereas a single authority has been introduced for several other important sectors such as the tax administration, the public prosecutor, the prison and probation administration and the social security administration. As the borders between authorities have been torn down it has become more important to introduce and enforce schemes for the internal access to personal data by the civil servants of the large, unified authority.

Due to the complexity and multitude of different provisions, it is not easy to get an overview of the existing special data protection legislation. There are, however, some common elements that have developed over the years and that nowadays usually appear in a special data protection act covering processing of personal data in a specific area of the public administration, although the wording or technical construction may vary between different acts.

Each act usually has some kind of definition of the *scope of application*. The construction of the definition varies considerably. Sometimes the act is said to cover processing of data carried out by authority X in its activities concerning Y, and sometimes it is said to cover processing of personal data on certain categories of persons, prisoners, for instance, in connection with the activities of authority X, the prison and probation administration, for instance. Other constructions are also prevalent. The definitions of the scope of application must be seen in connection with the provisions on the allowed purposes of the processing. Only processing operations carried out for the stated purposes are allowed according to the special data protection act and covered by that act.

General administrative activities, such as personnel management and administration, are routinely left outside the scope of application of the special data protection act, which means that processing of personal data in the course of those activities is covered by the general Personal Data Act.

Normally the same types of processing operations covered by the general Personal Data Act are covered by the special data protection act, i.e. wholly or partly automated processing (in computers) and other types of (manual) processing provided that the data processed is included in or is intended to form part of a structured collection of personal data that is available for searching or compilation according to specific criteria.

The Personal Data Act only covers processing of data on living individuals. The special data protection acts routinely cover processing of such data. According to some special data protection acts some provisions in the act are also applicable to processing of data on deceased persons or legal persons.

As regards the *relationship with the Personal Data Act*, the norm is that the special data protection acts complement the Personal Data Act and that that act is applicable insofar as there are no deviations in the special data protection act, but there have been some deviations from that norm.

There is routinely in the special data protection acts an explicit reference to the provisions in the Personal Data Act on rectification and damages. If the registration in a publicity register on, for example, ownership of real estate has legal effects, there are, however, often more elaborate provisions on the procedure for rectification in the act covering that particular register.

Sometimes, but not always, there is an explicit provision stating that the data subject has no right to object to the processing allowed under the special data protection act. In later years provisions have been introduced to the effect that processing that would not be allowed according to the legislation is permitted provided that the processing is done with the consent of the data subject.

There are as a rule no particular provisions on criminal sanctions for the infringement of the provisions in the special data protection acts. Non-compliance with the provisions by a civil servant can, however, result in criminal misuse of office, which is a punishable offence according to the penal code.

The Swedish Data Inspection Board has normally to supervise the application of both the Personal Data Act and the special data protection acts.

The special data protection acts routinely contain provisions on the *purposes for the processing*. It is not unusual to divide the purposes into two categories: Primary purposes and secondary purposes. The primary purposes are those purposes directly connected with the activities of the authority or authorities covered by the act. The tax authority may for instance process personal data for various defined purposes relating to the taxation activities carried out by that authority. The secondary purposes relate to the regulated authorities' function as suppliers of information needed by other authorities and make clear that data may also be processed for the purpose of provision of information to other authorities to be used by them for certain purposes. The tax authority may for instance process personal data for provision of information needed in activities, regulated by law, carried out outside the tax authority for the purpose of calculating pension benefits.

One purpose which is sometimes added to the list of purposes in the special data protection acts is the processing of data for checking, supervision, planning, evaluation and follow-up.

There is normally a provision in the special data protection acts on the *designation of the controller of the file, the data controller*.

The special data protection acts normally contain some provisions on the *categories of data that may be processed*. The act itself often contains provisions on when *sensitive personal data* as defined in article 8 in the directive, and the Personal Data Act, or *personal data on criminal offences* may be processed. Such data may often be processed if they have been submitted to the authority in



a specific case or insofar as they are necessary for the handling of a specific case. This means that the authority may process in a particular case incoming documents (e-mails or documents on paper which are scanned and put into an electronic document handling system) containing all sorts of data regardless if those data are necessary for the handling of the case, but that the authority itself may not create, or send out, a document containing sensitive personal data or personal data on criminal offences unless this is necessary for the handling of the case. There may also be other provisions allowing the processing of such data. More detailed provisions on which categories of sensitive personal data and other types of data may be processed are often found in a supplementing special data protection ordinance issued by the government in connection with the act.

Sometimes there are in the special data protection acts *provisions on a database*. The database is defined as a collection of data that, through automated means, are used jointly within the relevant sector of public administration. The database according to the definition may in fact consist of several different electronic systems, or computerised personal data files, which may or may not be interconnected or kept in a single, central computer. The content of the database is often further specified in a special data protection ordinance issued by the government in connection with the act.

There are often in the special data protection acts *provisions on limitations of what search criteria may be used*. Often these provisions limit, or even exclude, the use of sensitive personal data as a search criterion. This means in practice that it is not possible to compile a list of all data subjects sharing the same characteristics regarding sensitive personal data (a particular illness or ailment, for instance).

It is common to have provisions on *restrictions on external electronic access to the data* in the special data protection acts. External direct electronic access and disclosure of the data on an electronic media, such as a compact disc, is often restricted to a few authorities. More detailed provisions are often found in special data protection ordinances. Sometimes there are provisions explicitly allowing the data subject to have electronic access to his or her data.

The special data protection acts often contain provisions on *deletion* of the data. According to the Swedish legislation on public archives all official documents, including databases and other electronic material held by authorities, shall be archived and preserved unless there is a specific provision in the legislation or a decision by the Swedish National Archives (or, in some cases, the local government council) on deletion of the material. The provisions in the special data protection acts on deletion thus override the authorities' general obligation to archive and preserve. Since more and more official documents exist only in electronic format, an absolute provision requiring the deletion of the material would in the end lead to impoverishment of our national heritage as reflected by the preserved historical documents in archives. Provisions empowering the Swedish National Archive to prescribe exceptions therefore regularly supplement the provisions on deletion.

The construction of the provisions on deletion varies considerably. This is true as regards both the calculation of the retention period and the circumstances under which an exception to deletion may be prescribed.