FRA

Thematic Legal Study on assessment of data protection measures and relevant institutions Sweden

February 2009

Prof. Iain Cameron
Prof. Thomas Bull
Dr. Olle Mårsäter
Mr. Gustaf Almkvist
Mr. Love Rönnelid

Contents

EXECUTIVE SUMMARY **3**

1. Overview **4**

2. Data Protection Authority **8**

3. Compliance **11**

4. Sanctions, Compensation and Legal Consequences **15**

5. Rights Awareness **21**

6. Analysis of deficiencies **22**

7. Good Practice **25**

8. Miscellaneous **25**

ANNEXES **26**

Annexes ..... Error! Bookmark not defined.

Executive Summary

[1]. The main statute on data protection is the Personal Data Act (PDA, *personuppgiftslagen*) which was enacted in 1998 to bring Swedish law into conformity with the requirements of the Data Protection Directive 95/46/EC. However, other statutes regulate specific sectors, the police, the health sector etc.

[2]. The main oversight body established to maintain good standards of data protection in Sweden is the Data Inspection Board. The Board has several different powers in order to fulfill its tasks; it advises public and private sector actors on the law and good practice of data processing, it has a number of powers on delegation from the Government to regulate data processing and it can make inspections of both public and private entities. Such inspections can result in a decision noting deficiencies and specifying corrective measures. Furthermore, the authority issues permits to engage in certain types of sensitive data processing, it is the recipient of mandatory notifications in certain cases regarding automated handling of personal data and it receives individual complaints. It can issue a rectification order regarding inaccurate data, or to forbid further use of personal data if the handling is found to be in breach of the requirements of the PDA. Where the data handler does not comply with a rectification order, the Board may apply to the local administrative court to order the erasure of data.

[3]. The Data Inspection Board is regularly heard on all proposed legislation in the field. It has important educational and awareness-raising functions. The Board in fact mainly works by means of encouraging compliance, rather than "punishing" transgressors. Much data protection is at the level of "good practices" i.e. compliance with guidelines rather than strict legal requirements and rectification of inaccurate data. The Board considers that companies' compliance with guidelines and good practices is not always so strong, e.g. that they retain data for longer periods than the Data Inspection Board considers desirable. Still, in general the cooperative approach of encouraging compliance works well. There is an exception, however, the Data Inspection Board does not consider the possibilities to obtain compensation for wrongful data processing by private entities to be working satisfactorily. It claims that individuals are often deterred from claiming compensation by fear of high legal costs or by the long handling in the court system

[4]. There are few criminal cases before the courts. Civil claims against state agencies for compensation may be made directly to the

Chancellor of Justice who can decide to award compensation without court proceedings. In 2007 the Chancellor of Justice handled 54 claims concerned compensation according to the PDA for state processing of personal data contrary to the PDA. This system appears to work well.

[5]. Some of the discussion in Sweden has centred around the priority which tends to be given to freedom of information and freedom of expression over privacy concerns, however, this prioritizing cannot be said to be unpopular in Sweden. Commissions of inquiry are considering improvements in certain specific areas where data protection concerns have arisen, such as the health sector and employer access to work-place data.

[6]. There is a degree of disquiet in Sweden concerning increased police powers in the area of data processing, e.g. the use of biometric data in police work as well as the effects of EU measures in the area of harmonisation of police data and transboundary data flows.

1. Overview

[7]. Sweden's Constitution consists of four fundamental laws: the Instrument of Government, the Freedom of the Press Act, the Freedom of Expression and the Act of Succession. The first three documents all contain provisions directly or indirectly relevant to data processing. Chapter 2, section 3 of the Instrument of Government provides for a right to protection of personal integrity in relation to automatic data processing. This is, however, is only a framework right. The content of it is determined by statutory provisions (particularly the Personal Data Act, below) and government ordinances. The same article also provides for a prohibition on the (non-consensual) registration of persons purely on the basis of their political opinion. Chapter 8, sections 3 and 7 allow the parliament to delegate to the government (which may in turn delegate to administrative agencies) the power to make rules relating to data processing. The Freedom of the Press and Expression Acts provide inter alia for freedom of information and freedom of expression in the printed and electronic media. The constitutional status of these rights means that, when and if these come into conflict with privacy concerns, these rights tend to be given precedence (see further the next paragraph and section 6 below). A Commission of Inquiry has recently reported proposing that the right of personal integrity/privacy be explicitly written into the Instrument

of Government, thus giving it a similar status to the freedoms of expression and information.[1]

[8]. Sweden is a dualist state. The European Convention on Human Rights (ECHR) has been incorporated into Swedish law since 1995. The ECHR has, by virtue of Instrument of Government, Chapter 2, Section 23, a status between that of an ordinary statute and the Constitution. Sweden has ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) and its Additional Protocol regarding Supervisory Authorities and Transborder Dataflows (2001). These treaties have been implemented in Swedish law. Sweden has signed but not yet ratified the Convention on Human Rights and Biomedicine (1997). Sweden has ratified but not incorporated the International Covenant on Civil and Political Rights (ICCPR, 1966).

[9]. The Personal Data Act (PDA, *personuppgiftslagen*) was enacted in 1998 to bring Swedish law into conformity with the requirements of the Data Protection Directive 95/46/EC. The original statute was enacted in a hurry shortly after Sweden became a member of the EU. It has been subsequently amended on a number of occasions. Two of the more significant amendments made were in 2000, in order to align even closer to the EU Data Protection Directive standards on the transfer of personal data to third countries and in 2007, which exempted certain types of data from handling requirements in the PDA and replaced these with a simple rule designed to prevent the misuse of personal data. In addition to the PDA, there is also specific legislation regarding processing of personal data in a number of different sectors. These include the Patients' Data Act of 2008 (replacing earlier legislation from 1985 and 1998), the Police Data Act of 1998 and the Schengen Information System Act of 2000 (both currently in the process of being reformed),[2] the Land Register Act of 2000, and the Act on processing of personal data within Social Services of 2001. Other statutes which more indirectly deal with data protection include the Secrecy Act of 1980 (which regulates almost all types of official information which is to be kept secret), the Credit Information Act of 1973 (regulating procedures for checking creditworthyness), the Debt Recovery Act of 1974 and the Administrative Procedure Act of 1986 (governing procedures applicable to all administrative bodies). Government ordinances, issued either under inherent powers (Chapter 8, section 13 Instrument

[1] Skyddet för den personliga integriteten - Bedömningar och förslag, SOU 2008:3 http://www.regeringen.se/sb/d/108/a/96373 accessed 30th January 2009.

[2] A report on part of this process was recently presented, En mer rättssäker inhämtning av elektronisk kommunikation i brottsbekämpningen SOU 2009:1 http://www.regeringen.se/content/1/c6/11/91/63/bca06dc6.pdf accessed 30th January 2009.

of Government) or as a result of delegation by the parliament further specify data processing requirements.

[10]. The Directive on privacy and electronic communications (2002/58/EC) was largely implemented by the Electronic Communications Act (ECA) 2003.[3] The provisions dealing with unsolicited e-mail in the Directive were implemented in 2004 with amendments made to the Swedish Marketing Act which requires prior consent for direct marketing.[4]

[11]. The main oversight body in the field is the Data Inspection Board (see below, sections 2-4). The National Post and Telecom Agency is in charge of supervising compliance with the ECA, whereas monitoring of the Marketing Act, including the provisions on unsolicited e-mail, falls within the authority of the Swedish Consumer Agency.

[12]. As regards an overview on deficiencies and public debate, some of the discussion in Sweden has centred around the priority which tends to be given to freedom of information and freedom of expression over privacy concerns. Privacy International, for example, the international NGO concerned with promoting privacy concerns has "ranked" Sweden very low among EU states. Three points should be made here. First, the priority given to the freedoms of information and expression is not an error, or oversight, but largely the result of deliberate choice of the legislature. In some situations, the legislature must choose between these rights: it is not possible to respect both fully. Second, efficient use of benefits – informing people of what they are entitled to, and ensuring they obtain these entitlements – has been a part of the Swedish welfare state. This requires a high degree of access to information. Public authorities' access to information on people in Sweden has thus for a long time not been perceived as a problem by the great majority of the population. Thirdly, an area of concern in many countries has been employer access to personal data on its work-force. In Sweden, the work-place has been largely regulated by collective agreements between employer and employee organisations. The high degree of unionization in Sweden, and the relatively degree of high union input into the regulation of the work-place, means that – in most areas – this has not been a problem. However, Sweden is very much a part of a global economy, and privatization, diminished union power, changing corporate structures etc. mean that commissions of inquiry are presently considering whether improvements can be made in some specific areas, including protection of data in the work-place, (see below sections 4 and 6).

[3] Lag om elektronisk kommunikation, m.m. Prop.2002/03:110.
[4] Now in the Marknadsföringslagen (Marketing Act) SFS 2008:486.

[13]. It nonetheless cannot be said that data protection, in general, gives rise to much public concern in Sweden. As mentioned, the issue of police data protection is currently the subject of discussion. The Police data law is old. Simply put, the problem is that different data banks are kept separate (both in terms of local/national access and between different types of data banks – vehicle registers, convicted criminal registers etc). This makes it (deliberately) difficult to obtain a holistic picture. The question is how to ensure a high level of efficiency (which entails a broad group of operational police officers being given access to a broad spectrum of national data) at the same time as maintaining being high level of protection of personal integrity. While improvements are generally recognised to be necessary, certain specific police/security measures have given rise to particular discussion, indeed controversy. The first of these is the question of biometric data (discussed in section 6). The second is the implementation of the Data Retention directive.[5] A commission of inquiry has reported proposing how the Directive can be implemented.[6] The main criticism expressed by lawyers and the public has been of the directive, in that it requires a general (not targeted) retention of teledata. All traffic data generated in publicly available electronic communications, such as telephony or the Internet, would have to be retained by service providers for law enforcement purposes. The data would have to be kept for a minimum period of six months and a maximum period of two years. As it is this general retention which is the problem, the scope for avoiding or ameliorating privacy concerns in implementing the directive in national law is limited. A bill has not yet been laid before parliament on this issue. The third issue which has caused a major public controversy relates to data protection, but lies outwith the scope of the present report, namely the enactment of a statute permitting the Signals Intelligence Agency (Försvarets Radio Anstalt) to monitor and retain records of all cable borne telecommunications passing through Sweden.[7] Very unusually for Sweden, the bill was passed despite massive public protests. However, a proposal is to be laid before parliament later this year providing for improved safeguards.

[5] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

[6] SOU 2007:76, www.regeringen.se, accessed 26th January 2009.

[7] En anpassad försvarsunderrättelseverksamhet Prop. 2006/07:63.

2. Data Protection Authority

[14]. The Swedish Data Inspection Board (*Datainspektionen*) is an administrative agency with the main task of supervising the application of three laws concerning the handling of personal data. These laws are the Personal Data Act (1998) (PDA), The Debt Recovery Act (1974) and The Credit Information Act (1973). The authority has a budget of around 30 million SKR per year and employs around 40 people on a permanent basis. The authority has several different powers in order to fulfill its tasks; it advises public and private sector actors on the law and good practice of data processing, it has a number of powers on delegation from the Government to regulate data processing and it can make inspections of both public and private entities. Such inspections can result in a decision noting deficiencies and specifying corrective measures. Furthermore, the authority issues permits to engage in certain types of sensitive data processing, is the recipient of mandatory notifications in certain cases regarding automated handling of personal data and receives individual complaints.

[15]. As regards the powers required under the Directive 95/46/EC, first, the Data Inspection Board is regularly heard on all proposed legislation in the field. During 2007 representatives of the authority took part in eight committees drafting legislation and the Board was consulted formally 82 times on legislation involving, directly or indirectly, data processing issues. Secondly, it has powers to inspect public as well as private handlers of personal data and to issue a rectification order regarding inaccurate data, or to forbid further use of personal data if the handling is found to be in breach of the requirements of the PDA. Thirdly, where the data handler does not comply with a rectification order, the Board may apply to the local administrative court to order the erasure of data. The Board also has other powers as a result of the government ordinance on personal data (1998:1191). As regards the issue as to whether these powers are sufficient, in general the powers of the Board would seem to be satisfactory (although see further under 4 and 6 below). The Board does not, in practice, exercise an adequate degree of control over the accuracy of intelligence data collected by the police or the security police, as it lacks competence to evaluate this data. This was the main reason why the European Court of Human Rights considered that, in this area, the Board could not be regarded as an "effective remedy" within the meaning of Article 13 of the ECHR.[8] However, since 2008, this function is performed by another body, the Security

[8] Segerstedt-Wiberg and Others v. Sweden, No. 62332/00, 6 June 2006.

and Integrity Board (Säkerhets och integritetsnämnden, SIN, see further below section 7), which has the necessary competence and independence to perform this task. Where SIN finds that inaccurate data has been collected and retained, and in the unlikely event that the police or security police do not correct or erase this voluntarily, SIN can apply to the Data Inspection Board which can, if necessary by going to court, compel this correction or erasure.

[16]. It is noteworthy that although the Data Inspection Board has some quite useful tools at its disposal, the more far-reaching sanctions always involve a court. This is of course a limit to the remit of the Board, but one of great importance from a rule of law-perspective.

[17]. The budget has grown in the last years, while the number of staff has been rather stable for the last three or four years. There is no indication that lack of resources or personnel stops the Board from doing its duties.

[18]. In the Swedish constitutional document the Instrument of Government, national and local authorities are given an independent status in any individual case concerning application of law of use of public power (Ch 11:7 Instrument of Government). The tradition of strong administrative independence, going further than what the constitution actually proscribes, seem to guarantee that this constitutional regulation also works in practice.

[19]. The legal framework leaves it up to the Board to decide to what extent and in what forms its powers of inspection are to be used. The Board differentiates between three forms of inspections; field-inspections, desk-inspections and survey-inspections. Only the first kind is truly inspections on site, the others are more formal and based on documents and interviews, not physical observations. During 2007 the Board completed 38 field-inspections, 90 desk-inspections and 56 survey-inspections. This was a slight increase compared to 2006 and 2005. As for pro-active work, the Board uses several outreach tools for imparting to administrative agencies, companies and individuals, such as a web-site and a call-centre for those who have questions. The authority also organises conferences and educational activities (training courses etc.), especially for personal data representatives (see below, section 2). For example, amendments in the legislation during of 2007 led to an extra six conferences around the country to inform relevant people about the changes made.

[20]. Violations of the PDA come to the Board's attention in several ways, namely through individual complaints, inspections and a formalized consultation procedure. The Board has discretion to decide which

complaints to pursue, however, complainants are always notified as to whether an investigation is started, and if so, its outcome. In 2005, the Board handled 405 complaints about personal data processing, and in 2006 307 complaints (see further, appendix 1). In its annual report for 2007, the Board notes that individual complaints now play a smaller role than before in obtaining an overview of how compliance is working in practice, while the importance of the consultation procedure had grown.[9] The consequence was that there were fewer findings of violations as such, but investigation work took up more resources than expected, as cases were complicated.

[21]. The Board publishes a selection of its decisions on its web-site. It is decisions concerning the PDA that the Board has found to be of most interest to the public. Furthermore it publishes rather extensive reports on topical themes as guidance and these guides seem to build on existing cases as well as, obviously, the law. All decisions – even unpublished decisions - are available on request, according to the rules in the constitution on access to public documents.

[22]. The Opinions of the Working Party established under the Directive are not considered as binding when it comes to the interpretation of the Swedish law, but they are certainly a tool for inspiration. The authors of the leading commentary on the legislation refers to the Working Party in their book.[10] Few cases have reached the Swedish courts (see below, section 4), and these seem to rest their decisions on the Swedish preparatory works and the rulings of the ECJ.

[23]. As noted above, the Board is very active in legislative procedures and has been consulted on around 80 draft bills a year for some time.[11]

[24]. The Board mainly uses mass-media contacts and its own information tools (web.site, printed information, etc.) in order to raise awareness of the problems around protection of personal integrity.

[9] *Datainspektionen, Årsredovisning 2007* [Annual Report 2007]. Available online at http://www.datainspektionen.se/Documents/arsredovisning-2007.pdf, accessed January 29th 2009.

[10] Öman, Sören, Lindblom, Hans-Olof, *Personuppgiftslagen. En kommentar*, 3rd ed., Norstedts Juridik 2007.

[11] See, e.g. the Board's opinions on the law on strategic surveillance http://www.datainspektionen.se/Documents/remissvar/2009-02-24-signalspaning.pdf, and on the government approval of the Council decision on Europol, http://www.datainspektionen.se/Documents/remissvar/2008-07-02-europol.pdf.

3. Compliance

[25]. As regards notification of processing of personal data, according to Section 36 (1), PDA, the controller of personal data shall notify the Data Inspection Board of the processing of all personal data that is completely or partially automated. The notification shall be made in writing, and signed by the data controller or an authorized representative before processing is undertaken. Notifications shall, according to Section 6, DIFS 2001:1[12], contain: "(a) the name, address, telephone number and registration number of the data controller; (b) the purpose or purposes of the processing operation; (c) a description of the category or categories of data subjects affected by the data processing; (d) a description of the category or categories of data concerning the data subjects that are to be processed; (e) details of the recipients or categories of recipients to whom the data may be disclosed; (f) information concerning data transfer to third countries; (g) a general description of the measures that have been taken to safeguard the security of processing operations." The same Section also state that changes in the above mentioned circumstances shall be notified in the same way as the original notification.

[26]. The above mentioned notification need not be made if the controller of personal data has appointed a personal data representative and notified the Data Inspection Board of who he/she is.[13]

[27]. According to Section 36 (3), PDA, The Government or an authority appointed by the Government may issue regulations concerning exemptions to the notification duty referred to in the first paragraph, as long as the processing will not result in an improper intrusion of personal integrity. The Government has under this section issued exemptions to the notification duty regarding:

a. (1) the processing of personal data that is undertaken pursuant to an authority's obligation under Chapter 2 of the Freedom of the Press Act to provide official documents; (2) the processing undertaken by the archive authority pursuant to the provisions of the Archives Act (1990:782) or the Archives Ordinance (1991:446); (3) the processing governed

[12] Regulation amending data Inspection Board Regulation (DIFS 1998:2) with regard to the obligation to notify the processing of personal data to the Data Inspection Board.
[13] Section 37, Personal Data Act (1998:204).

by specific regulations in a statute or enactment in other cases than those mentioned in items (1) and (2).[14]

b. processing personal data in running text or unstructured material (Section 5 (a) PDA).[15]

c. processing of sensitive personal data that is performed under Section 17[16] of the Personal Data Act (non-profit organisations); nor does the duty of notification apply to the corresponding processing by such an organisation of other kinds of personal data than sensitive personal data.[17]

[28]. In addition to the above mentioned exceptions from the requirement of notification, exceptions are also made in cases when the data subjects have consented to the processing of personal data,[18] or in cases when the data controller, in processing of personal data, keeps a record of processing operations involving data that would otherwise have been subject to notification. The later cases are, according to Section 5, (DIFS 2001:1):

a. (a) personal data relating to data subjects who are associated with the data controller by reason of membership, employment, a customer relationship or similar relationship, provided that the processing does not relate to sensitive data within the meaning of section 13 of the Personal Data Act;

b. (b) health data kept by employers that relate to workers' sick leave periods, provided that the data are used for salary administration purposes or to determine whether the employer is required to undertake a rehabilitation investigation;

c. (c) personal data kept by employers that reveal workers' trade union membership, provided that the data are used to enable employers to fulfil obligations or exercise rights under labour law or to make it possible to determine, enforce or defend legal claims;

[14] See Section 3, Personal Data Ordinance (1998:1191), as amended.
[15] Section 4, Personal Data Ordinance (1998:1191), as amended.
[16] "Non-profit organisations with political, philosophical, religious or trade union objects may within the framework of their operations process sensitive personal data concerning the members of the organisation and such other persons who by reason of the objects of the organisation have regular contact with it. […]"
[17] Section 5, Personal Data Ordinance (1998:1191), as amended.
[18] Section 4, Regulation amending data Inspection Board Regulation (DIFS 1998:2) with regard to the obligation to notify the processing of personal data to the Data Inspection Board, (DIFS 2001:1).

d. (d) personal data collected from data subjects where processing is essential for compliance with the provisions of laws or regulations;

e. (e) personal data the processing of which is permitted in the health sector under section 18 of the Personal Data Act;

f. (f) personal data used in the activities of lawyers that are relevant to the provision of their services and to measures to avoid conflicts of interest; and

g. (g) personal data processed under sector-wide agreements reviewed by the Data Inspection Board pursuant to section 15 of the Personal Data Ordinance (1998:1191). (DIFS 2001:1).

[29]. As regards compulsory notification of particularly privacy-sensitive processing of personal data**,** according to Section 41, PDA, the Government may issue regulations providing that such processing of personal data as involves particular risks for improper intrusion of personal integrity shall be notified in advance. The government has specified in the above ordinance that notification must be made to the Data Inspection Board in these cases three weeks before data processing begins. This is to enable the Board to check routines, safeguards etc. For these cases the above mentioned exemption from the obligation to notify (which applies after the appointment of a personal data representative, Section 37, PDA) is not applicable.

[30]. According to Section 10 of the Personal Data Ordinance (1998:1191), the processing of personal data on genetic predispositions, which have been observed through testing, must be notified according to the above mentioned procedure. Provisions relating to prior notification are also contained in section 2 of the Police Data Ordinance (1999:81), section 2 of the Processing of Personal Data in Connection with Tax Authorities' Involvement in Criminal Investigations Ordinance (1999:105) and section 2 of the Processing of Personal Data in the Law Enforcement Activities of the Swedish Customs Ordinance (2001:88).[19]

[31]. Notifications for the purposes of prior checks by the Data Inspection Board shall be made in writing and signed by the data controller or the authorized representative. Notifications

[19] Section 1, Regulation amending data Inspection Board Regulation (DIFS 1998:2) with regard to the obligation to notify the processing of personal data to the Data Inspection Board, (DIFS 2001:1).

shall contain the information specified in section 6 and the reasons why it is necessary for the Data Inspection Board to carry out a prior check. Notifications shall also include details of the scheduled date for commencement of the processing operation and a contact person who can supply information. As regards notifications for the purposes of prior checks pursuant to section 10 of the Personal Data Ordinance (1998:1191), these shall also contain: (a) details whether the processing has been checked by a research ethics committee and if so, a copy of the committee's decision; (b) information, where appropriate, that the data subject has consented and (c) a description of the information to be given to the data subject. Any change in the above circumstances shall be notified in the same way.[20]

[32]. As regards data protection officers **t**he duties of the "personal data representative" (*personuppgiftsombud*) is independently to ensure that the controller of personal data (*personuppgiftsansvarig*) processes personal data in a lawful and correct manner and in accordance with good practice. The personal data representative shall also point out any observed inadequacies. If the personal data representative has reason to suspect that the controller of personal data contravenes the provisions applicable for the processing personal data, and if rectification is not implemented as soon as possible after being brought to the attention of the controller, the personal data representative shall report this situation to the Data Inspection Board. The personal data representative shall also consult with the Data Inspection Board in the event of doubt about how the rules applicable to processing of personal data shall be applied.[21] In 2006, the number of personal data representatives was 3,284, down from 3,420 in 2005, although having said that, representatives can represent several entities.[22] In April 2007 the Data Inspection Board had been notified of the appointment of some 3 300 personal data representatives by approx. 5 800 controllers of personal data.[23]

[33]. There is no obligation to appoint a personal data representative. According to Section 36 (2) of the PDA, the controller of

[20] Section 7, Regulation amending data Inspection Board Regulation (DIFS 1998:2) with regard to the obligation to notify the processing of personal data to the Data Inspection Board, (DIFS 2001:1).
[21] Compare Section 38, Personal Data Act (1998:204).
[22] Datainspektionen, *Årsredovisning 2006*, p. 22 http://www.datainspektionen.se/Documents/arsredovisning-2007.pdf, accessed 29 January 2009.
[23] Petersson, Roger, Reinholdsson, Klas, *Personuppgiftslagen i praktiken*, 4th ed., Norstedts Juridik 2007. p. 86.

personal data shall notify the Data Inspection Board if the controller appoints or discharges a personal data representative. Notifications shall include the names of the data controller and the personal data representative and be made in writing and signed by the data controller or its authorized representative.[24]

[34]. The personal data representative shall be a natural person. The requirement in Section 38 PDA that the personal data representative shall act independently means that the representative should not have an overly subordinate position in relation to the controller of personal data. The representative can be employed by the controller, but must be able independently to carry out his or her mandate under the PDA. In order to protect the representative in the fulfilment of his or her duties, the employer cannot normally subject the representative any to any negative consequences usually applicable under labour law (dismissal, reprimand, salary reduction etc.).[25]

[35]. There are no requirements in the PDA for the representative to have special qualifications or to undergo special training in matters relating to the processing of personal data and protection of privacy,[26] but the Data Inspection Board state that it aims for a high level of knowledge of the representatives. The Data Inspection Board gives advice and support, and also provides training for the representatives. During 2007, ten courses at three different levels were organized specifically for representatives. Representatives have a special contact officer at the Data Inspection Board, who answers questions by telephone and e-mail. When a new representative is notified to the Data Inspection Board, he or she is provided with a specially designed binder containing information and regulations.[27]

4. Sanctions, Compensation and Legal Consequences

[36]. The consequences of processing personal data contrary to the Personal Data Act (PDA) can be divided into two categories:

[24] Section 8, Data Inspection Board Statute Book (DIFS 2001:1).
[25] Government Bill, Personal Data Act, Proposition. 1997/98:44, p. 138-139.
[26] Öman et al. op. cit., p. 406; Petersson, Roger, Reinholdsson, Klas, *Personuppgiftslagen i praktiken*, 4th ed., Norstedts Juridik, 2007. p. 88.
[27] Datainspektionen, *Årsredovisning 2007*, p. 19. http://www.datainspektionen.se/Documents/arsredovisning-2007.pdf, accessed 29 January 2009.

consequences intended to ensure rectification of the non-compliance with the rules (PDA sections 43- 47), and consequences related to the injury caused (sections 48 and 49). Most other acts regulating the processing of personal data in specific fields refer to the PDA when it comes to the regulation of rectification and compensation, e.g. the Police Data Act [*polisdatalag*, 1998:622] and the Patients' Data Act 2008 as well as numerous other acts regulating the processing of personal data in various other government agencies and certain private institutions.[28]

[37]. In order to achieve compliance, the Data Inspection Board is entitled to full insight into the data processed, whether or not there is any suspicion of non-compliance (PDA section 43). If the Board wishes to take further action, or establishes that data is processed or might come to be processed contrary to the PDA, it is to inform the responsible party and demand rectification. It may also prescribe a default fine in order to achieve rectification or to limit processing to storage (sections 44 and 45).

[38]. The Board may also apply at the County Administrative Court for personal data processed contrary to the PDA to be erased. Erasure may not be decided if considered unreasonable (section 47).

[39]. An individual whose personal data has been processed contrary to the PDA shall be compensated by the responsible controller of personal data for both the damage and for the violation of personal integrity that the processing contrary to the regulations in the Act has caused (section 48). The responsible controller is typically a state body or a company, but can also be another type of association or an individual (cf. section 1).

[40]. The individual only needs to prove causation, i.e. that the *processing* that has been conducted *in violation of the PDA* has caused the damage and/or the violation of personal integrity. The individual is thus not required to provide evidence of mens rea, such as intent or negligence. This fact, in particular when combined with the fact that it is not necessary to prove that economic damage has been caused, illustrates that the right to compensation fulfils not only a reparatory but also a punitive role.[29]

[41]. Under the PDA, compensation can be awarded not only for processing explicitly contrary to the PDA, but also for processing contrary to "good practice" (as laid down in sections 9). What

[28] For a comprehensive list, see Öman, S & Lindblom, H-O, *Personuppgiftslagen: en kommentar*, Stockholm, 2007, pp.32-43.
[29] Cf. *Personuppgiftslagen: en kommentar*, p. 436.

constitutes good practice is, however, not stated in the Act, and the *travaux préparatoires* consider it a task for the Courts and the Data Inspection Board to establish the contents of the term. [30]

[42]. Compensation according to section 48 can be awarded for damage to personal integrity, physical damages as well as for damages to goods. It may also be awarded for non-pecuniary damage, an extension of the right to compensation available through the Torts Act [*skadeståndslag*, 1972:207], under which a right to compensation only exists if the non-pecuniary damage is caused by a criminal act. Similarly, the right to compensation due to violation of personal integrity is broader than the similar right in the Torts Act which again depends upon a crime having been committed.[31]

[43]. While the right to compensation for processing of personal data contrary to the PDA does not require proof of intent or negligence, the liability of the controller of personal data to pay compensation may be adjusted under certain circumstances (section 48, para 2), to the extent that it is considered reasonable in the individual case. Such adjustment can entail that no compensation is actually paid.

[44]. The circumstances that may ground a possibility of adjustment are not immediately clear from a reading of the PDA. The directive (95/46/EC) states that the controller should prove that "he is not ***responsible*** for the event giving rise to the damage" (art 23, para 2). The meaning of "responsibility" is ambiguous, as it can mean either that the controller did not cause the event or that the event lay outside of his sphere of legal responsibility. The travaux préparatoires to the PDA attempt to solve the issue by indicating that if a breach of the law has been shown to have occurred, and this has harmed the complainant in some way, the onus of proof is on the controller to show that s/he was not responsible for the breach of the law. If s/he succeeds with this, it is up to the court (or the Chancellor of Justice, see below) to determine whether this should lead to a reduction in compensation and if so, by how much.[32]

[45]. Under certain circumstances the right of the individual to economic compensation is supplemented by a penal sanction (section 49), in which case intent or gross negligence must be manifested. Apart from the case where untrue information is provided regarding the contents of personal data processed or when personal data is transferred to a third country in breach of the PDA, the criminal

[30] Prop. 1997/98:44 *Personuppgiftslag*, p. 108.
[31] *Personuppgiftslagen: en kommentar*, p. 440.
[32] The Swedish Council on Legislation [*Lagrådet*] in its preview of the PDA criticized the ambiguity in Prop. 1997/98:44 *Personuppgiftslag*, bilaga 7, pp. 248-249.

sanctions mainly concern cases when personal data that has been deemed particularly sensitive is processed contrary to the PDA. As indicated earlier, it is thus forbidden, though with certain exceptions, to process personal data containing information on e.g. race, political or religious orientation or membership of a trade union. The punishment is a fine or a maximum six months imprisonment. In petty cases no sentence shall be imposed, while grave cases may entail up to two years imprisonment.

[46]. The only cases regarding the PDA that have been heard by the Supreme Court [*Högsta domstolen*] have so far been criminal cases. In NJA 2001 s 409, which concerned events soon after the PDA entered into force, the Court made clear that personal data that has been processed for journalistic purposes is excluded from the application of the PDA. The defendant had published personal information about senior bank managers on a website highly critical of corporate culture and influence of the Swedish banks. The Supreme Court considered that the rules of the Freedom of Expression Act went before the PDA. This meant that the defendant should have been charged, if at all, with the offence of defamation. When this offence is committed in the electronic media in certain conditions (as applied here) it could only be prosecuted under the FOE Act. It accordingly acquitted the defendant on the charges of violation of the PDA.

[47]. Another interesting case when it comes to the application of the penal sanction is NJA 2005 s 361, where the Court discussed, inter alia, the meaning of "petty cases" [*ringa fall*] (section 49, para 2). A school board had published on their website a letter to the parents of pupils complaining about difficulties in co-operating with an employee who had then been granted sick-leave. Referring to the ECJ ruling C-101/01, the majority of the Court considered the importance of freedom of speech as well as the interest of the individual in having his private life protected, and ruled that the publication of the letter was not a "petty case". Supreme Court Justice Victor, one of the Court's leading criminal lawyers, dissented opinion and argued that the publication was a petty case. Seeing that the publication was not criminal under any other legislation, only the primary purposes of the PDA ought to be considered when deciding what cases that are "petty". As the publication had been a single instance, and not part of a systematic campaign, Justice Victor considered it to be a "petty case".

[48]. In one published case the defendant has been sentenced to imprisonment. In the Court of Appeals case RH 2002:71. A man had published adverts for sexual contacts together with photos of his ex-girlfriend. This act, which constituted not only a crime against the

PDA but also defamation of his ex-girlfriend, led to three months imprisonment and a 100 000 SEK compensation for violation of personal integrity.

[49]. As stated above, the Data Inspection Board has certain powers that it may use in its supervisory role, mainly the prescription of a default fine to achieve compliance or application to the relevant Country Administrative Court for an erasure order regarding data processed contrary to the PDA. The Board also exercises its supervisory role in preventive activities, such as giving lectures, providing guidance and presence in the media. It also inspects organisations processing personal data.

[50]. Inspections by the Data Inspection Board can be caused by information in the media, focal efforts of the Board or by individual complaints. In 2007 226 such complaints were received, while 167 inspections of different kinds were initiated.[33] Complaints can be put forward and advice can be given by contacting the Board Call Centre. The opinion of the Board is that in such cases where the responsible controller wishes to rectify his mistake, as often is the case after inspections, the supervisory role works well.[34]

[51]. As regards government or administrative agency processing of data, under the Decree (1995:1301) on the Handling of Claims against the State for Compensation [*förordning (1995:1301) om handläggning av skadeståndsmål mot staten*] claims against the state for compensation may be put forward to the Chancellor of Justice [*justitiekanslern*], who can decide to award compensation without court proceedings. In 2007 the Chancellor of Justice handled 1166 such claims in total, of which 54 claims concerned compensation according to the PDA section 48 for state processing of personal data contrary to the PDA.[35] In a number of these cases the Chancellor of Justice has awarded compensation. Recent cases in which compensation has been awarded include a mix up of health information between two personal files at the Social Insurance Agency (JK dnr 1604-06-40), incorrect information on the date when a withheld driving license should be returned (JK dnr 1127-05-42), and the publication of a court ruling stating the name of an employee

[33] Datainspektionen, *Årsredovisning 2007* [Annual Report 2007], pp. 8-14. Available online at http://www.datainspektionen.se/Documents/arsredovisning-2007.pdf, accessed January 24th, 2009.

[34] Datainspektion, *Yttrande*, dnr 446-2008, June 4th, 2008. Available online at http://www.datainspektionen.se/Documents/remissvar/2008-06-16-remissvar-integritetsskyddskommitten.pdf, accessed January 24th, 2009.

[35] Justitiekanslern, *Årsredovisning för Justitiekanslern 2007* [Annual Report for the Chancellor of Justice 2007]. Available online at http://www.jk.se/arsredovisning/2007/arsredovisning%202007.pdf, accessed January 24th, 2009.

on the intranet of the Prison and Probation Service (JK dnr 2370-04-42). Several cases where personal data had been processed incorrectly as a result of incorrect information being registered to begin with (as a result of the fault of the data subject) have not led to compensation being awarded according the PDA (eg JK dnr 3672-03-42).

[52]. Overall, the Swedish system of sanctions, compensation and legal remedies must been seen as focused on rectification of processing of personal data contrary to the PDA rather than on compensation and other sanctions. There have been only a few cases of compensation and sanctions according to the PDA in the Supreme Court (see above). The Data Inspection Board is of the opinion (see above) that the right to compensation against private entities is not being claimed in the courts to the extent that it should (see below, section 6). With the Board taking mainly a supervisory role based on achieving rectification, the possibility to be awarded compensation by the Chancellor of Justice is relatively efficient and without the risk of heavy costs for the applicant, but this only exists when the responsible controller is a state body.

[53]. While the Board often successfully asks processors of personal data that are suspected of acting contrary to the PDA to rectify their behaviour voluntarily, the Board does not provide legal assistance for seeking compensation in the courts. It does, however, provide some legal advice through its call centre. In criminal cases the case is handled by a public prosecutor, in which case the prosecutor shall also prepare and present the aggrieved person's action in conjunction with the prosecution, provided that no major inconvenience will result and that the claim is not manifestly devoid of merit (Code of Judicial Procedure [*rättegångsbalken*, 1942:740], Chapter 22, Section 2). It is thus mainly in cases of compensation that are not based on criminal behaviour (cf PDA sections 48 and 49) and which are not directed against the state that the plaintiff has to carry the financial risk. In certain cases it is possible, however, to obtain financial assistance under the Legal Aid Act [*rättshjälpslagen*, 1996:1619]

[54]. There is no specific legislation in Sweden related to the protection of personal data in the context of employment, which means that it is the PDA that applies to such cases. Several government committees have discussed whether specific legislation should be adopted, in particular in SOU 2002:18, which includes a draft of a possible Act on the Protection of Personal Integrity in Professional Life [*lag om skydd för personlig integritet i arbetslivet*] This has not led to any legislation being passed. Instead a new government committee on the

same topic has been appointed.[36] This committee has seen its duration prolonged several times, and is now due to present its conclusions no later than April 15th, 2009.[37] In its directives the government mentions the need to establish clear rules concerning e.g. computer usage, e-mail, logging of electronic locks and digital storage of CCTV footage.

[55]. Much of the work of the Data Inspection Board has concerned the context of employment. Other than diverting resources to this field and receiving and investigating complaints, as explained above, the protection of personal data in employment is not ensured in any particular way. While many trade unions provide legal advise to their members, such aid is mainly related to Labour Law. The trade unions are not given any formal role in ensuring compliance with the PDA, nor do questions of personal integrity and data protection at work seem to have been a priority among the Swedish trade unions in later years.

5. Rights Awareness

[56]. The Data Inspection Board regularly surveys different public and private sectors, as well as groups in society. Three recent reports can be mentioned. The first relate to provincial health authorities' levels of awareness of data protection rules relating to accessibility to patients' data.[38] The survey was prompted by a number of incidents in which health workers uninvolved in a particular case had nonetheless obtained sensitive data concerning patients and, in some cases, leaked this to the media. The Board considered that there were considerable differences in how health authorities handled the issue (see also below, section 6). A second survey which can be mentioned was a questionnaire sent to 103 companies and public authorities, chosen at random, regarding employer's attitudes towards employees use of the Internet and e-mail and the monitoring that exists by means of processing of biometric data and surveillance cameras.[39] A third recent study on awareness of, and attitudes towards, data

36 Dir. 2006:55, *Personlig integritet i arbetslivet*.
37 Dir. 2008:152, *Tilläggsdirektiv till Utredningen om integritetsskydd i arbetslivet (N 2006:07)*.
38 Summary in English available at Report 2005:1 http://www.datainspektionen.se/Documents/rapport-accessibility-to-patients-data.pdf, accessed 29th January 2009.
39 Monitoring in Working Life Report 2005:3, English summary available at http://www.datainspektionen.se/-Documents/rapport-monworklife-summary.pdf accessed 27th January 2009

protection law and rights in the population was made of young people, ordered by the Data Inspection Board.[40]

6. Analysis of deficiencies

[57]. The major public debates recently on data protection and related matters have already been referred to in section 1. This section will sketch out some of the other deficiencies in Swedish data protection. There is little wrong with the Data Inspection Board as such, or the guidelines it produces. However, implementation of these can be deficient at times. In Sweden, central government is small and public administration is decentralized. The majority of public administration is performed by local authorities. Independent administrative agencies are also responsible for much public administration. Each administrative authority and local authority is in law quite separate from each other, with its own data systems. Data-matching gives rise to concerns, but it can be necessary for a variety of reasons: efficiency, preventing benefit or tax fraud, crime investigation etc. The organizational separation of public administration means that, even though everyone has a personal identification number, data-matching is made more difficult. However, for a variety of reasons, temporary shortages of funds, loss of experienced staff, delays or problems in introduction of computer systems, the authority in question may temporarily fail to meet the data protection requirements set out in the PDA, or in Data Inspection Board guidelines. An example of this is the already mentioned (above section 5) report into health workers' access to patient's data. Allowing all health workers access to all patient data increases efficiency, and helps in cases of medical emergencies, when time counts. However, it also means that more people have access to sensitive data (meaning a greater infringement of personal integrity) as well as increasing the risks of leaking of sensitive data. The Data Inspection Board stated in this respect that it should be possible to vary the accessibility in regard to the need of information a certain official may have. The accessibility can be decided with the basis of for example position, medical specialisation and established co-operation. Divisions that regularly co-operate because they belong to the same organization normally should be able to get access to one another's information, assuming that the secrecy issues have been solved. There must also be efficient tools for follow-up and traceability. The identification of the user must comply with security restrictions.

[40] http://www.datainspektionen.se/Documents/rapport-ungdom-2009.pdf.

[58]. Another deficiency already mentioned is that the Data Inspection Board works mainly by means of encouraging compliance, rather than "punishing" transgressors. The remedy which it can provide is largely limited to rectification of inaccurate etc. data. However, much data protection is at the level of "good practices" i.e. compliance with guidelines rather than strict legal requirements and rectification of inaccurate data. The Board considers that companies' compliance with guidelines and good practices is not always so strong, e.g. that they retain data for longer periods than the Data Inspection Board considers desirable.[41] Still, in general the cooperative approach of encouraging compliance works well. There is an exception, however. In certain circumstances – which are probably increasing in modern society – compensation is necessary. This can be quickly and cheaply obtained from the public sector, through the Chancellor of Justice. However, the Data Inspection Board does not consider the possibilities to obtain compensation for wrongful data processing by private entities to be working satisfactorily. It claims that individuals are often deterred from claiming compensation by fear of high legal costs or by the long handling in the court system.[42] Bearing in mind the significance of large private companies and the data they hold and collect, this is, at least potentially, a large deficiency in data protection. The Swedish society is not "legalized" in the sense of encouraging dispute settlement in the courts. This is a good thing, but it may be that, in the future, improved legal aid will be necessary to ensure that compensation is obtainable for people whose personal integrity has been infringed by a company.

[59]. As regards the issue of work-place data privacy, the above mentioned (section 5) survey by the Data Inspection Board revealed few very serious problems. Biometric data was not been used to any significant degree. However, the Data Inspection Board did express some criticism regarding camera surveillance. The Board did not consider it enough to put up signs in the spaces where the camera surveillance is carried out, which was the case among some of the employers in this study. Moreover, it was still common that employers do not have any procedures when it comes to deleting data in accordance with the Personal Data Act. The Data Inspection Board considered that data that is the basis of the employer's monitoring of the employee's use of the Internet and e-mail in

[41] See, e.g. the Board's report on Bonus cards and the Personal Data Act Report 2005: http://www.datainspektionen.se/Documents/rapport-bonus-cards.pdf accessed 25th January 2009.

[42] Datainspektionen, *Årsredovisning 2007* [Annual Report 2007], pp. 8-14. Available online at http://www.datainspektionen.se/Documents/arsredovisning-2007.pdf, accessed January 24th, 2009.

normal cases should not be kept longer than three months. It is likely that the Board's views will be incorporated into whatever legislative proposals might eventually be made to regulate this area.

[60]. Another area, which is related to the area of study, but involves so many other issues that it is better not to discuss it here outside of it is the question of protection of copyright. Parliament has recently adopted amendments to the law allowing the owners of copyright (particularly in films and music) to have access to internet providers' data in order to determine which internet users are illegally file-sharing. This has been a very controversial issue in Sweden, and one which has particularly engaged young people.

[61]. Finally, as already mentioned in section 1, there is a degree of disquiet in Sweden concerning EU measures in the area of harmonisation of police data and transboundary data flows.[43] The Police Data Act, as already indicated, is overdue for an overhaul, and is in the process of being reformed. Another, related area of discussion, although it would be too strong to say controversy, is biometric data in police work. According to current legislation, DNA samples fall under the rules in Chapter 28 of the Code of Judicial Procedure and rules in the Police Data Act of 1998. The inquiry which reviewed the current legislation suggested introducing specific rules regarding DNA samples in law enforcement and allowing such samples to be taken from persons who are arrested, taken into custody, or suspected of crimes that can lead to imprisonment[44], but also from other persons if it is required in the investigation of such crimes. According to the inquiry's report, results from DNA analyses should be put into the DNA register kept by the National Police Board regarding persons who are suspected of, or sentenced for, crimes where the penalty includes imprisonment. The present rules on the DNA register are relatively restrictive. These allow registration of those who have been *convicted* of a crime that involves a penalty of more than two years' imprisonment. According to Section 24 of the present Police Data Act, registration must be limited to such data that provides information about identity. Other DNA information must not be registered. The inquiry suggested that information in the register should be deleted when the preliminary investigation is withdrawn or when charges against the individual in question have been withdrawn or rejected.

[43] See e.g. the Data Inspection Board's critical report on implementation of Prüm treaty http://www.datainspektionen.se/Documents/rapport-prumfordraget.pdf accessed 25th January 2009.

[44] Genetiska fingeravtryck Ds 2004:35, http://www.regeringen.se/sb/d/108/a/27189 accessed 20th January 2009.

[62]. In conclusion, the problems identified above are relatively minor. They are only partly the result of deficiencies in legislation. Swedish legislation in this field often has an international or EC/EU origin. At times the need for this legislation has only been accepted reluctantly in Sweden, such in the area of file-sharing and copyright protection. Here, the "problem" is a lack of real democratic support for the legislation penalizing breaches of copyright, and this in turn can reduce the authorities' willingness to prioritize enforcement. Other problems of an occasional lack of coordination between administrative agencies are an inevitable price one pays for the decentralized system of administrative agencies. Other problems can be traced to a lack resources.

7. Good Practice

[63]. The Data Inspection Board's website (which also contains basic documentation on Swedish laws and guidelines in English) is accessible and easy to follow. The Board's successful educational and awareness raising activities are also "good practice".[45] Another good practice is the creation of the Security and Integrity Board, which provides an expert, and independent, remedy for people worried that the police may be unlawfully collecting, or retaining security or policing data.[46]

8. Miscellaneous

[64]. Nothing to report.

[45] For general information on the Personal Data Act in English see http://www.datainspektionen.se/Documents/faktabroschyr-behandling-ju-eng.pdf accessed 25th January 2009

[46] http://www.sakint.se/Startsida.html, accessed 12th January 2009.

Annexes

Annex 1 - Tables and Statistics

Please complete the table below[47]

	2000	2001	2002	2003	2004	2005	2006	2007
1. Budget of data protection authority (in thousands of SEK)								
a) Government grants	27412	29493	32734	29427	30276	29450	28596	32539
b) All revenues	28712	31701	34746	31080	31629	30762	31622	34924

[47] All information gathered from the official reports of the Data Inspection Board. Available online at http://www.datainspektionen.se/ladda-ner-och-bestall/informationsmaterial/arsredovisningar/, accessed January 29th.

2. Staff of data protection authority	37	43	40	39	40	40	44	41
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative[48]	-	-	-	-	-	-	-	-
Number of data protection registrations (*anmälningar)*	242	846	332	209	193	169	215	180
Number of data protection approval procedures								
"Precontrol" according to the Personal Data Act (*förhandskontroll)*	77	92	174	200	132	127	153	240
Permission according to Credit Information Act	7	1	8	4	5	5	4	5
Permission accordning to Dept Recovery Act	38	52	40	55	50	44	50	39

[48] The official statistics from the Data Inspection Board does not discern between how procedures are being initiated. On the contrary, it states that the inspections mentioned in the statistics are initiated by individual complaints, due to media reports and at the Boards own initiative. The number of different investigations stated at the end of the table.

Sum	**122**	**145**	**222**	**249**	**187**	**176**	**207**	**284**
Number of complaints received by data protection authority								
Personal Data Act	166	272	406	421	450	450	307	226
Data Act	189	69	-	-	-	-	-	-
Credit Information Act	125	91	81	81	68	78	63	48
Dept Recovery Act	196	226	224	750	309	286	284	246
Sum	**676**	**658**	**711**	**1252**	**827**	**814**	**654**	**520**
Number of complaints upheld[49] by data protection authority	-	-	-	-	-	-	-	-

[49] The official reports of the Data Inspection Board does not include any statistics on the results of their investigations. However, all complaints are stated to receive some kind of answer by the Board, e.g. *Datainspektionen, Årsredovisning 2007* [Annual Report 2007], p. 14. Available online at http://www.datainspektionen.se/Documents/arsredovisning-2007.pdf, accessed January 29th.

Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)[50]	-	-	-	-	-	-	-	-
Sanctions and/or compensation payments in data protection cases (please disaggregate between court, data protection authority, other authorities or tribunals etc.) in your country (if possible, please disaggregate between sectors of society and economy)[51]	-	-	-	-	-	-	-	-
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)[52]	-	-	-	-	-	-	-	-
Number of inspections started concerning the Personal data act Field inspections	76	95	160	116	90	45	52	33

[50] No statistics available.
[51] No statistics available.
[52] No statistics available.

Desk inspections	-	-	-	-	-[53]	74	85	79
Questionnaire inspections	51	30	90	184	26	104	10	55
Sum	-	-	-	-	-	**243**	**147**	**167**
Number of supervision matters [*tillsynsärenden*] started concerning the Credit Infromation Act	-[54]	25	39	33	29	34	15	18
Out of which inspections	-	3	6	8	2	4	1	3
Number of supervision matters [*tillsyns*ärenden] started concerning the Dept Recovery Act	167	176	179	161	171	130	153	100
Out of which inspections	41	47	35	25	29	23	59	20
Number of matters [*ärenden*] finished concerning the Personal Data Act (and the Data Law 2000 and 2001)	219	235	324	251	407	310	112	184

[53] No official statistics available concerning Desk Inspections until 2005.
[54] No statistics available for year 2000.

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

Case title	NJA 2001 409
Decision date	June 12th 2001
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Case nr B 293-00 by the Supreme Court of Sweden *(Högsta domstolen).*
Key facts of the case	A businessman had published texts on Swedish bank employees and corporate culture on the internet. The express purpose of the webpage was to criticize the actions of Swedish banks and corporations. The texts included personal

(max. 500 chars)	records for 71 persons in alphabetical order. The texts were partly factual but subjective, highly critical, commentary was also included. The question in the case was whether the publication of this information was criminalized under the Personal Data Act (PDA), and especially if it could be subsumed under the exception for "exclusively journalistic purposes" *(uteslutande journalistiskt syfte)*.
Main reasoning/argumentation (max. 500 chars)	The Supreme Court describes the background of the PDA in order to clarify its subsequent reasoning. It states that since the PDA is an implementation of an EC-directive it has to be interpreted in line with it. With reference to article F.2 of the former TEU, the Court considered that the directive in turn has to be interpreted in the light of the ECHR. The court considered the exception from punishable scope for information with "exclusively journalistic purposes" is to be seen as aimed at resolving the same kind of conflict that can occur between article 8 and 10 ECHR. Conflicts are to be resolved by applying the principle of proportionality and striking a fair balance between competing concerns, bearing in mind each state's margin of appreciation. The court held that the expression "journalistic purpose" not only protects journalists working for the mass media but also everyone's right to bring matters of concern to the general public. The information's character, not the quality is to be judged. In this case that meant that the information on the homepage fell within the exception. Where information published constituted the crime of defamation the option of bringing a prosecution for this was always possible.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The case lays down essential interpretive lines by stressing the legislations connection with the ECHR. The main precedent however is the interpretation of the conjunction "exclusively for journalistic purposes", which is an exception from penal sanction. The court finds that journalistic purposes is a broad concept, which's aim is to guarantee a general free dissemination of information. The word "exclusively" is found to be a special reduction of the exception when media processes certain information without an informational intention, e.g. direct advertisement and the handling of subscriptions.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The accused was found not guilty.
Proposal of key words for data base	Journalistic purpose, Internet, Dissemination of information, Penal sanction.

Case title	NJA 2005 s 361
Decision date	May 26th 2005
Reference details (reference number; type and title of	Case B 3042-03 by the Supreme Court of Sweden *(Högsta domstolen).*

court/body; in original language and English [official translation, if available])	
Key facts of the case **(max. 500 chars)**	The case concerns a teacher in a Swedish boarding school, who after having reported in a local newspaper about alleged bullying on the school was given sick-leave. The school, in an official e-mail letter to the parents, stated that the teacher had been transferred due to "co-operational problems" *(samarbetssvårigheter)* and that he had been sick-listed for the past week.
Main reasoning/argumentation **(max. 500 chars)**	First, the court found that the law explicitly states that an approval to publication of personal information has to be left in advance. The court found the information to be sensitive. In the final question (which the court went into most detail on) the court discussed the scope of "petty cases", which is an exception from criminalisation. The majority (four out of five judges) held that whether information is to constitute a "petty case" is to be judged on the basis of a cumulated evaluation of all circumstances in the particular case, e.g. the information's nature, the kind of integrity violation or the risk for integrity violation. With regard to the parents 'legitimate interest in their children's' situation, that the information had been on the internet for four weeks, that it had not been removed immediately when requested and the not insignificant violation of integrity, the court found the information not to constitute a "petty-case".
Key issues (concepts, interpretations) clarified by	1. An approval to publishing of certain information must be left in advance, not afterwards. 2. The scope for health information to be considered sensitive is broad. 3. When information is published on the internet, it is not considered

the case (max. 500 chars)	spread to a third country if the internet provider is established in the member state or in another member state. 4. Whether a case is considered a "petty-case" and thereby not a criminal offence is to b judged on the basis of a cumulated evaluation of all circumstances in the particular case, e.g. the information's nature, the kind of integrity violation or the risk for integrity violation.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The case resulted in 40 heavy fines on 1000 SEK each, i.e. 40 000 SEK.
Proposal of key words for data base	"Petty-case", Sensitive information, Internet, the Swedish Personal Data Act, Third country.

[65]. Please attach the text of the original decisions in electronic format (including scanned versions as pdf).