FRA

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

Turku, Finland
March 2009

Contents

Executive summary

Overview

General legal framework

[1]. The constitutional standards for data protection in Finland are based on Section 10 of the Finnish Constitution,1 which explicitly mentions the protection of personal data. In addition, the European and international human rights standards have a direct significance for domestic measures relating to personal data. Ordinary legislation on the protection of personal data is currently based on the Personal Data Act (Henkilötietolaki, Personuppgiftslag Act no. 523/1999).2 In addition, there are several sector-specific laws on data protection.

Data Protection Authority

[2]. There are two data protection authorities in Finland: The Data Protection Board [hereinafter: the DPB, or the Board] and the Data Protection Ombudsman [hereinafter: the DPO, or the Ombudsman]. The powers given to the data protection authorities correspond to the requirements of Article 28 of Directive 95/46/EC.

[3]. The DPB is the primary decision-making authority in data protection issues in Finland, although it only makes a few decisions annually. The role of the DPO is primarily preventive and guidance-oriented. Conversely, the reactive mechanisms have a minor significance. The DPO plays a significant advisory role in preparation of legislative or administrative reforms. The DPO also has a major role in awareness raising through active participation in public discussions as well as active policy of information dissemination.

[4]. The resources allocated to the data protection authority have thus far been sufficient for ensuring the effective use of the powers given to the data protection authority. Similarly, the guarantees of independence granted to the data protection authorities in Finland are principally sufficient to ensure effective use of the powers given to the data protection authority. However, the situation may be changing to the worse because the tasks and responsibilities of the DPO are steadily increasing whereas the current Finnish Government's

1 Unofficial English translation of the Constitution of Finland is available at: http://www.finlex.fi/en/laki/kaannokset/1999/en19990731 (28.11.2008).
2 Unofficial translation available at http://www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf (01.12.2008).

Productivity Programme only allows half the jobs vacated by natural attrition to be filled.

Compliance

[5]. General framework regarding duties of registration of data processing operations is defined in the Personal Data Act (PDA). The supervision of compliance is carried out by data protection authorities and mainly through notification and permissions procedures as well as orders and inspections.

[6]. There are widening discrepancies in compliance between private and public sector. The most serious instances of lack of compliance have concerned the two largest telecommunications companies in Finland, Nokia and Sonera.

Sanctions, Compensation and Legal Consequences

[7]. Although existing legislation provides for criminal sanctions relating to data protection violations as well as for compensatory damages, these consequences are uncommon. Similarly, the follow-up activities do not represent significant part of practices of data protection authorities in Finland because the Office of the DPO emphasises the prevention of violation as a primary duty. The protection of personal data collected and processed in the context of employment is mainly provided by the Act on the Protection of Privacy in Working Life.

Rights Awareness

[8]. The studies on the awareness of data protection issues suggest that, in comparison to other EU countries, a somewhat smaller proportion of population is suspicious of issues relating to personal data protection. However, the studies also reveal that a significant number of people have nevertheless experienced at least some sort of infringement of their rights.

Analysis of Deficiencies

[9]. The following deficiencies exist. First, the constitutional standards involving protection of personal data still remain somewhat underdeveloped in the domestic constitutional practice. Second, as the domestic system of data protections relies on preventive and legally somewhat soft methods of

supervision, such as guidance, already occurred abuses of rights are left without appropriate legal treatment. Third, the legislation concerning data protection is widely dispersed in different sector-specific laws.

Good Practices

[10]. It is submitted that the following features can be regarded as constituting good practices. First, the protection of personal data features as an autonomous fundamental right under Section 10 of the Constitution. Second, the explicated purposes of the existing legislation as well as the standards used for its interpretation are conscientiously tied to fundamental rights and international human rights. Third, the Finnish DPO has embraced a particularly wide and energetic approach to proactive measures obtainable for the development and supervision of data protection legislation.

1. Overview

[11]. The following section provides for the legal framework of domestic system of data protection. It will first introduce the constitutional doctrine as well as the relevant and domestically applicable international standards. After addressing the deficiencies identified in the national debate on data protection, the section will conclude by an overview of data protection legislation, relevant institutions and other relevant instruments in Finland.

1.1. Constitutional standards

[12]. The primary constitutional standards relevant for data protection in Finland are based on Section 10 of the Finnish Constitution (Suomen perustuslaki, Finlands grundlag, Act no. 731/1999)3. which provides for explicit protection of personal data, among others:

[13]. "Everyone's private life, honour and the sanctity of the home are guaranteed. More detailed provisions on the protection of personal data are laid down by an Act.

[14]. The secrecy of correspondence, telephony and other confidential communications is inviolable.

[15]. Measures encroaching on the sanctity of the home, and which are necessary for the purpose of guaranteeing basic rights and liberties or for the investigation of crime, may be laid down by an Act. In addition, provisions concerning limitations of the secrecy of communications which are necessary in the investigation of crimes that jeopardise the security of the individual or society or the sanctity of the home, at trials and security checks, as well as during the deprivation of liberty may be laid down by an Act."4

[16]. Accordingly, Section 10 of the Constitution enumerates the general right to privacy as well as more specific privacy related guarantees.

[17]. As with constitutional rights in general, these rights may conflict with other fundamental rights. In terms of data protection, the most obvious candidate in this respect is laid down in Section 12 of the Constitution, which provides for freedom of expression as well as for the principle of openness and the right to access government documents.

---

3 Unofficial translation is available at http://www.finlex.fi/fi/laki/kaannokset/1999/en19990731.pdf (28.11.2008).

4 Unofficial English translation of the Constitution of Finland is available at: http://www.finlex.fi/en/laki/kaannokset/1999/en19990731 (28.11.2008).

[18]. Although right to privacy as well as other constitutional rights mainly aim to protect the individual against arbitrary interference by the public authorities, they do not merely compel the public authorities to abstain from such interference. Instead, Section 22 of the Constitution, which requires that all public authorities guarantee the observance of constitutional and international human rights, is also understood to entail positive obligations to the state and public authorities in general.5 As the most authoritative interpreter of Finnish Constitution, the Constitutional Law Committee, has often emphasized, Section 22 sets forth obligations to adopt measures designed to secure respect for private life and personal data also in the horizontal relations between private parties.6

[19]. The most explicit constitutional guarantee for the protection of personal data is provided by the second sentence of Section 10 subsection 1 of the Constitution as follows: "More detailed provisions on the protection of personal data are laid down by an Act". Since the constitutional mandate to enact detailed legislation is unqualified, and since the provision does not enumerate a specific right to personal data protection, the wording leaves a fairly large margin of appreciation for legislator.

[20]. However, the travaux préparatoires of the Fundamental Rights reform of 1995 already make a reference from the personal data clause of Section 10 to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) (Finnish Treaty Series 35–36/92), which requires a certain minimum standard for all legislation concerning personal data.7 Similarly, the Constitutional Law Committee has regarded this Convention as laying the minimum standard of data protection.8

[21]. Moreover, the Constitutional Law Committee has frequently9 stated that although leaving a certain margin of appreciation for the legislator, constitutional obligation on protection of personal data must nevertheless be read in its wider constitutional context. Accordingly, the Committee has interpreted the personal data clause in conjunction with right to privacy and required that it be ensured in a manner that conforms to the domestic system for the protection of fundamental rights as a whole.

---

5 See, for instance the Government Bill 309/1993 (fundamental rights reform), p. 75.

6 See, for instance Finland/Perustuslakuvaliokunta/PeVL 9/2004. Subsequently, PeVL is an abbreviation for an Opinion by the Constitutional Law Committee. The reports and opinions by the Constitutional Law Committee of Parliament are available at: http://web.eduskunta.fi/Resource.phx/valiokunnat/valiokunta-pev01/index.htx?url=/plaza/toimielimet/muut/zvkseuraavakokous_pev01_su.html&te=pev01&lmg=fi (28.11.2008).

7 See, the Government Bill (309/1993 vp) on amending the provisions on fundamental rights (HE 309/1993 vp), p. 53.

8 See, e.g., opinions PeVL 26/1996vp and 28/1997vp.

9 See, e.g., opinions PeVL 11/2008 vp, p. 3/I, PeVL 27/2006 vp, p. 2/I, PeVL 2/II, PeVL 6/2003 vp, p. 2/I, PeVL 51/2002 vp, p. 2/I and PeVL 14/2002 vp, p. 2/I of the Constitutional Law Committee of Parliament.

[22]. These constitutional principles have concretised as fairly precise constitutional requirements for personal data legislation. The Constitutional Law Committee has demanded all legislation on personal data to include detailed and conclusive provisions on the purpose for which the data is collected. Moreover, also the permissible content of collected and registered information and the permissible uses of collected data including its disclosure to third parties must be legislated with equal conclusiveness and detail. Duration of the registration and due process rights of registered persons must also be precisely regulated.10 However, the doctrine is still somewhat immature leaving the practice to a certain extent incoherent and incomplete.11

[23]. Notwithstanding the deficiencies in the doctrine, the doctrine nevertheless has had positive effects on the constitutional protection of personal data. The constitutional requirements developed by the Constitutional Law Committee have been applied to both public authorities and private entities. Furthermore, the transfer of personal data between different authorities has been regulated according to same principles. Finally, the Constitutional Law Committee has consistently maintained that processing of sensitive personal data such as information regarding health, criminal susceptibility and involuntary treatment, falls into the core of the right to privacy. Therefore, "such legislation must be precise".12

[24]. Although the standard model of review involving data protection legislation does not include a genuine proportionality test, analogous approach is occasionally used. For instance, the Constitutional Law Committee has required the personal data originating from confidential communications is to be grounded on necessity requirement.13 Similar necessity requirement is applied to such inter-administrative disclosure legislation that does not conclusively limit the content of transferrable personal information. However, if the personal data being transferred between authorities is conclusively defined in the law, the disclosure may be grounded merely on the need of authority in question.

[25]. Besides these direct constitutional standards for the protection of personal data, the data protection issues have gained indirect support from other aspects of constitutional rights in general and rights to privacy and the secrecy of confidential communications in particular. In fact, Constitutional Law Committee of Parliament usually defines the data protection issue in terms of both the right to privacy in general and the special clause requiring protection of personal data by an act in particular. Similar overlap is typical to cases that concern restrictions on the right to secrecy of confidential communications, which characteristically involve some kind of processing of private information, thus making the measures relevant in terms of personal data protection.

10 See, e.g., opinions PeVL 32/2008 vp and PeVL 11/2008 vp.
11 Compare, for instance, opinions PeVL 7/2000, 23/2006 vp and PeVL 18/2008.
12 See, PeVL 25/1998 vp.
13 See, PeVL 18/2008 vp.

[26]. In these cases, the standard of constitutional review usually turns out to be stricter than in the case the measures under review fall solely under the specific clause on data protection under Section 10, subsection 1 of the Constitution.

[27]. To sum up, although the wording of the data protection clause in the Finnish Constitution implies fairly limited constitutional protection for the guarantees of personal data, the actual constitutional practices have followed a somewhat stricter standard. However, the doctrine is still somewhat underdeveloped. The Constitutional Law Committee of Parliament seems to adhere to several different standards in relation to data protection. In one strand of the cases it aims to draw clear distinction between rights pertaining to personal data protection and other privacy rights thus leaving the legislator a wider margin of appreciation. In the other end, data protection is approached as a genuine right that relates to right to privacy and may be restricted only under the same strict conditions as rights in general are. These incoherencies can be explained partly also by the ambiguities relating to the very concept of data protection. If understood in a strict sense, it covers only protection of personal data. If understood in the wide sense, it covers also a wide variety of privacy relevant rights such as rights to confidential communications, data protection and so forth.

1.2. European and International Standards

[28]. In addition to constitutional principles, European and international human rights standards for data protection have a direct significance for domestic measures relating to personal data. As a matter of Finnish constitutional law, regional and international human rights treaties and other instruments feature as minimum standards of protection. This constitutional premise also applies to various human rights instruments on data protection.

[29]. Finland has ratified, among others, the following human rights treaties that have relevance upon data protection issues. The reference to Finnish Treaty Series (FTS) indicates the year of their entry into force in domestic law:

- The European Convention on Human Rights (1950, FTS 18–19/1990).
- The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981, FTS 35–36/1992).
- The International Covenant on Civil and Political Rights (1966, FTS 7–8/1976).

[30]. However, Finland has ratified neither the Convention on Human Rights and Biomedicine (1997)14 nor the Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding Supervisory Authorities and Transborder Dataflow (2001) yet.15

[31]. The status of these human rights guarantees within the national legal order is defined by four distinct, yet inter-related elements. First, unlike the other Nordic countries, and except for a few cases, Finland usually incorporates human rights treaties into its domestic law, thereby making them directly applicable by the courts and public authorities.

[32]. Second, due to the fact that Section 22 of the Finnish Constitution requires all public authorities to observe, not only constitutional rights, but also human rights, all constitutional guarantees of personal data are directly supported by respective provisions in international human rights law and the EU Charter of Fundamental Rights. Furthermore, this constitutional duty under Section 22 to enforce international human rights treaties applies equally to all public authorities, including the judiciary.

[33]. Third, since the Constitutional Law Committee of Parliament is under obligation to review legislative proposals and other matters brought for its consideration in relation to both, the Constitution and international human rights treaties (Section 74 of the Constitution of Finland), the Committee ought to review all legislative measures concerning data protection in terms of both constitutional and international human rights standards. In practice, conformity with international human rights standards is occasionally reviewed.

[34]. Fourth, the constitutional doctrine is that international human rights obligations binding upon Finland feature as a minimum standard of protection for the equivalent rights under the Constitution of Finland. Thus, public authorities are actually under a constitutional duty to try to provide higher or more extensive protection to various rights under the Constitution of Finland.

[35]. Finally, it is to be emphasised that aside from international human rights, EU law also provides legal background for domestic data protection legislation. Indeed, the existing Finnish legislation on data protection is largely based on EU directives. Moreover, as illustrated by the recent judgment of the Court of Justice in Case C–73/07 (*Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy*), EU law is also capable of providing the criteria for distinguishing between right to data protection and freedom of expression.

---

14 See, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=164&CM=&DF=&CL=ENG (27.11.2008).

15 See, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=&CL=ENG (27.11.2008).

1.3. Data Protection Legislation

[36]. Legislation on the protection of personal data was originally issued in 1987 by Personal Data File Act (*Henkilörekisterilaki*, *Personregisterlag*, Act no. 471/1987) which was later replaced by Personal Data Act[16] (*Henkilötietolaki*, *Personuppgiftslag* Act no. 523/1999, hereinafter the PDA). The PDA accommodates the reform of the fundamental rights provisions of the Finnish Constitution in 1995 and the EU Data Protection Directive (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).

[37]. The PDA aims to implement, in the processing of personal data, the protection of private life and the other fundamental rights which safeguard the right to privacy, as well as to promote the development of and compliance with good processing practice. Being applicable to all processing of personal data, unless otherwise provided elsewhere in the law, it functions as a general law of data protection in Finland. The Act includes detailed provisions regarding processing of personal data, sensitive data and personal identity number, processing of personal data for special purposes, transfer of personal data to outside the European Union, the data subject's rights, including the rights concerning access and rectification, as well as provisions concerning data protection authorities, data security and storage of personal data, direction and supervision of the processing of personal data together with miscellaneous provisions concerning liability in damages and criminal sanctions.

[38]. The Act on the Openness of Government Activities[17] (*Laki viranomaisten toiminnan julkisuudesta, Lag om offentlighet i myndigheternas verksamhet*, Act no. 621/1999) provides for a general right to access any official document in the public domain held by public authorities, including electronic records.

[39]. The Act on the Protection of Privacy in Electronic Communications[18] (*Sähköisen viestinnän tietosuojalaki, Lag om dataskydd vid elektronisk kommunikation*, Act no. 516/2004) intends to ensure confidentiality and protection of privacy in electronic communications. The Act implements Directive 2002/58/EC of 12

[16] Unofficial translation available at http://www.finlex.fi/fi/laki/kaannokset/1999/en19990523.pdf (01.12.2008).
[17] Unofficial translation available at http://www.finlex.fi/fi/laki/kaannokset/1999/en19990621.pdf (01.12.2008).
[18] Unofficial translation available at http://www.finlex.fi/fi/laki/kaannokset/2004/en20040516.pdf (01.12.2008).

July 2002 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector. Since its enactment, the Act has been revised (Act no. 343/2008) to implement 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.

[40]. Moreover, Parliament is currently considering amendment to the Act, which would specify and clarify the rights of companies to process e-mail identification data. According to the Bill, companies will be given a right to process identification data in their communications networks to detect, prevent and investigate violations of business secrets, unauthorized use, espionage as well as certain other crimes. In its recent opinion that has been heavily criticised both by constitutional experts and the media[19] the Constitutional Law Committee of Parliament approved the bill.[20]

[41]. Act on the Protection of Privacy in Working Life[21] (*Laki yksityisyyden suojasta työelämässä, Lag om integritetsskydd i arbetslivet*, Act no. 759/2004) lays down provisions on the processing of personal data about employees, the performance of tests and examinations on employees and the related requirements, technical surveillance in the workplace, and retrieving and opening employees' electronic mail messages.

[42]. Finally, various sector specific laws include provisions concerning data-protection. Representative examples are Health Care Professionals Act[22] (*Laki terveydenhuollon ammattihenkilöistä, Lag om yrkesutbildade personer inom hälso- och sjukvården*, Act no. 559/1994) which contains provisions on the retention of patient documents and their confidentiality (Section 16) and on the obligation of secrecy (Section 17) as well as Acts on the Status and Rights of Patients[23] (*Laki potilaan asemasta ja oikeuksista, Lag om patientens ställning och rättigheter*, Act no. 785/1992) and on the Status and

19 See, for instance 'Legal experts say "Lex Nokia" violates constitution', published in *Helsingin Sanomat*. Available at http://www.hs.fi/english/article/Legal+experts+say+%E2%80%9CLex+Nokia%E2%80%9D+violates+constitution/1135241264898 (01.12.2008).

20 See, PeVL 29/2008 vp.

21 Unofficial translation available at http://www.finlex.fi/fi/laki/kaannokset/2004/en20040759.pdf (01.12.2008).

22 Unofficial translation available at http://www.finlex.fi/fi/laki/kaannokset/1994/en19940559.pdf (01.12.2008).

23 Unofficial translation available at http://www.finlex.fi/fi/laki/kaannokset/1992/en19920785.pdf (01.12.2008).

Rights of Social Welfare Clients (*Laki sosiaalihuollon asiakkaan asemasta ja oikeuksista, Lag om klientens ställning och rättigheter inom socialvården*, Act no. 812/2000), which lay down the key legal principles concerning the legal protection of patients and social welfare clients, including the protection of their personal information.

1.4. Data Protection Authorities

[43]. The existing legislation sets forth two public authorities for the supervision of data protection legislation in Finland. These are *the Data Protection Ombudsman [DPO]* and *the Data Protection Board [DPB]*.

[44]. The DPO provides direction and guidance on the processing of personal data, supervises the processing, in order to achieve the objectives of the Personal Data Act (PDA), and makes decisions concerning right of access and rectification.

[45]. The DPB deals with questions of principle relating to the processing of personal data, where these are significant to the application of the PDA. The DPB may grant permission for the processing of personal data, if the processing is necessary, otherwise than in an individual case, in order to protect the vital interests of the data subject, or to use the public authority of the controller or a third person to whom the data is to be disclosed. Moreover, if measures of guidance and advice have failed to remedy a given situation, the DPO may, in certain cases, bring an act of violation to the consideration of the DPB.

2. Data Protection Authority[24]

[46]. As noted above, there are two data protection authorities in Finland: the DPO and the DPB. The Personal Data Act (PDA) provides for the legal basis of both the authorities.

[47]. The DPO is an independent authority affiliated to the Ministry of Justice. The office is run by the DPO, appointed by the Council of State for a term of five years. The current DPO has held the office since 01.11.1997. The total number of staff is 20. The current budget of the Ombudsman's office is approximately EUR 1.5 million.25

[48]. Similarly, the DPB is an independent authority affiliated to the Ministry of Justice. It consists of a chair, deputy chair and five members, who are required to be familiar with register operations. The Board is appointed by the Council of State for a term of three years.

[49]. The DPB is the primary decision-making authority in data protection issues. It may grant permission for the processing of personal data, if the processing is necessary, otherwise than in an individual case, in order to protect the vital interests of the data subject, or to use the public authority of the controller or a third person to whom the data is to be disclosed. The permission may be granted also in order to realise a legitimate interest of the controller or the recipient of the data, provided that such processing does not compromise the protection of the privacy of the individual or his/her rights. The Board may also grant permission for the processing of sensitive data, for reasons pertaining to an important public interest and for either a fixed period of time or for the time being. And finally, the DPB has also to issue an order in specific cases provided by Section 44 of the PDA and explained below.

[50]. During 2007, the Board convened six times and decided six cases. Of those, five concerned data protection permissions and one orders. This amount of activities is typical for the Board. Hence, its role is rather passive.

[51]. Compared to the Board, the role of the DPO is much more active. Moreover, although the role of the Ombudsman is primarily preventive and guiding in nature, it has also been entrusted with some decision-making and consultative powers. The DPO provides controllers and data subjects with guidance and advice on request, and makes decisions pertaining to the compliance with legislation and implementation of the rights of data subjects. In matters concerning the implementation of the right of verification and the correction of

[24] Information included in this part of the report is largely based on an interview with the Finnish DPO, held in the premises of DPO's office 03.12.2008.

[25] See, Finland /Tietosuojavaltuutetun toimintakertomus *2007*, p. 8 (2007 financial report of the DPO). Available in Finnish at: http://www.tietosuoja.fi/uploads/w8a22r.pdf (23.11.2008).

personal data, the decisions of the Ombudsman are binding and subject to appeal. Moreover, the public prosecutor must consult the DPO prior to bringing charges based on violations of the Personal Data Act. Courts of law are also obliged to provide the Ombudsman with an opportunity to be heard in cases concerning related issues. In both cases, the Ombudsman provides statements.

[52]. Furthermore, according to Section 39 of the PDA, regardless of confidentiality provisions, the DPO has the right of access to personal data, which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data. The DPB has the same right in matters which it is dealing with.

[53]. Finally, the DPO has the power to inspect personal data files and to assign experts to carry out the inspection. For purposes of the inspection, the DPO and an expert have the right to enter the premises of the controller and a person operating on the behalf of the controller, where personal data are processed or personal data files are kept in such premises, and to access the information and equipment required for carrying out the inspection.

2.1. Conformity of the Powers of the Data Protection Authorities with Article 28 of the Data Protection Directive

[54]. The powers given to the domestic data protection authorities are designed to correspond to the requirements of Article 28 of Directive 95/46/EC.

[55]. Corresponding requirements set forth in Article 28 paragraph 2, the consultation in the preparation of regulation or the adoption of measures is guaranteed in Section 41 of the PDA. According to Section 41 subsection 1, the authority concerned shall reserve the DPO an opportunity to be heard in connection with the drafting of legislative or administrative reforms relating to the protection of personal rights or freedoms in the processing of personal data. Moreover, subsection 2 requires that before bringing charges for conduct contrary to the PDA, the public prosecutor shall hear the DPO. When hearing a case of this sort, the court shall reserve the DPO an opportunity to be heard.

[56]. The investigative powers, which are meant in Section 3(2) of Article 28 of the Data Protection Directive are given to the data protection authorities by Section 39 of the PDA which provides for data protection authorities' right of access and inspection. These powers include, among others, the DPO's right of access to personal data

which are being processed, as well as all information necessary for the supervision of the legality of the processing of personal data. These rights exist regardless of confidentiality provision. Moreover, the DPB has the same right in matters which it is dealing with. In addition, the Ombudsman has also the right to inspect personal data files and to assign experts to carry out the inspection and for purposes of the inspection, the DPO and an expert have the right to enter the premises of the controller and a person operating on the behalf of the controller.

[57]. In terms of effective powers of intervention, as provided by Article 28, paragraph 3(2) of the Data Protection Directive, Section 44 of the PDA lays down the main provisions. Accordingly, at the request of the DPO, the DPB may:

a) prohibit processing of personal data which is contrary to the provisions of the Personal Data Act or the rules and regulations issued on the basis of the Act;

b) in matters other than those concerning right of access or rectification, compel the person concerned to remedy an instance of unlawful conduct or neglect;

c) order that the operations pertaining to the file be ceased, if the unlawful conduct or neglect seriously compromise the protection of the privacy of the data subject or his/her interest or rights, provided that the file is not set up under a statutory scheme; and

d) revoke a permission granted by the Board, where the prerequisites for the same are no longer fulfilled or the controller acts against the permission or the rules attached to it.

[58]. If a personal data file is no longer necessary for the operations of the controller, Section 34 of the PDA requires it to be destroyed, unless specific provisions have been issued by an Act or by lower-level regulation on the continued storage of the data contained therein or the file is transferred to be archived.

[59]. In terms of procedural guarantees, as provided by Article 28, paragraph 3(3), the powers to engage in legal proceedings are laid down in Sections 40, 45 and 46 of the PDA. According to Section 40, the DPO may refer the matter to be dealt with by the DPB, or report it for prosecution. Section 45 concerns the rights to appeal and Section 46 provides for threat of a fine, which the DPO may impose in order to reinforce the duty to provide access to data. The DPB may do likewise in relation to the duty to provide access to data.

[60]. The procedural guarantees of data subjects (Article 28 Section 4 of the Data Protection Directive) are provided by Sections 28 and 29 of the PDA. According to Section 28, the data subject may bring the matter to the attention of the DPO in cases where the controller has refused to provide access to the data. Section 29 gives the data subject a right to bring the case into the attention of the DPO if the controller refuses to rectify an error in a personal data file. These rights apply also to situations covered by Article 13 of the Data Protection Directive.

[61]. The interview with the DPO revealed that the powers given to the data protection authorities are sufficient to ensure effective data protection in Finland.

2.2. The Remit of the Data Protection Authorities

[62]. The remit of the data protection authorities in Finland is notably wide — especially with regard to the DPO. There are no apparent limitations that would be inconsistent with the substance and supervisory functions of the authority in question.

[63]. According to Section 40 of the PDA, the DPO shall promote good processing practice and issue directions and guidelines so as to achieve a situation where unlawful conduct is not continued or repeated. Hence, the primary duty of the DPO is to influence, in advance, compliance with the legislation concerning the keeping of registers. In addition to general guidance, the DPO also:

- provides controllers and data subjects with guidance and advice on request;
- provides guidance and consultation in the compilation and review of field specific Codes of Conduct;
- provides consultations and statements for authorities, prosecutors and courts of laws in matters relating to application of data protection legislation;
- assesses compliance with the law of data processing through inspections; and
- makes decisions pertaining to the compliance with legislation and implementation of the rights of data subjects.

[64]. The remit also includes international cooperation. The Finnish DPO is a member of the consultative, independent working group of national Data

Protection Ombudsmen provided for in the EU Data Protection Directive (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). In addition, the Finnish DPO is a member of the joint supervisory bodies included in the Europol and the Schengen agreements.

[65]. In contrast, the remit of the other data protection authority, i.e. the DPB, is noticeably limited both in scope and in practical relevance. The Board is a decision-making authority, which makes no more than ten decisions yearly. The small number of decisions is related to narrow mandate as the Board only has two functions both relating to more or less extreme cases in the area of data protection. First, the DPB grants permissions for the processing of personal data mainly in cases concerning sensitive data and other interests of the data subject, or a third person. Second, the DPB may issue orders but only at the request of the DPO. Hence, it provides a sort of a "last resort" mechanism for data protection. However, its decisions usually relate to issues of principle, which raises their qualitative importance.

2.3. Resources and Independence

[66]. Until now, the resources allocated to the data protection authorities have been sufficient for ensuring the effective use of the powers given to the data protection authority. The budget of DPO's office is approximately 1,5 million euros. However, the situation is getting worse. The yearly increases in the budget of DPO's office have been marginal not alowing for increases in the size of the staff. At the same time, the tasks and responsibilities of the DPO have been steadily rising during the last years. Moreover, the Finnish Government's Productivity Programme seeks to increase the productivity and efficiency of central government so that by allowing only half the jobs vacated by natural attrition to be filled. Hence, it can be expected that the budgetary resources allowed for DPO's office will shrink at the same time as the duties continue to expand. In fact, both the National Audit Office of Finland and the Law Committee of Parliament have recently required more resources to be given to the DPO's office as well as an establishment of new office of Deputy to the DPO.26 Accordingly, without appropriate budgetary measures, the effective supervision of data protection will be at risk in Finland. Due to the limited role of the DPB, these problems do not affect its role in a similar manner.

[26] See, Opinion 15/2008 of the Law Committee of Parliament. Available in Finnish at http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/lavl_15_2008_p.shtml (15.12.2008). See also National Audit Office of Finland's Performance Audit Report 161/2008, The development and use of identification services in public administration, pp. 171–172. Available at http://www.vtv.fi/chapter_images/8463_161_2008_Tunnistuspalvelut_NETTI.pdf (15.12.2008) . English abstract available at http://www.vtv.fi/chapter_images/8465_1612008_Identification_services.pdf (15.12.2008).

[67]. The guarantees of independence granted to the data protection authorities in Finland are principally sufficient to ensure effective use of the powers given to the data protection authority. However, and related to the growing resource problems, the fact that both the DPO and the DPB are operating under the Ministry of Justice, which makes the decisions on the budget, might present problems also in terms of independence. On the other hand, based on the interview with the DPO, these worries have remained on theoretical level. Similarly, there have been no attempts by interest groups to influence the data protection authorities.

2.4. Powers Relating to Own Initiatives

[68]. The PDA does not include provisions explicitly requiring the DPO to become active on its own initiative. However, as the Act puts emphasis on the preventive measures and aims, these powers can be deemed to exist. Different types of inspections are one form of self-initiated activity.

[69]. The powers relating to inspections are laid down in Section 39 of the PDA. Although inspections are regularly used to monitor compliance of data protection legislation, the number of yearly inspections implies it to be of minor significance compared to other forms of data protection supervision. For instance, in 2007, the DPO made only 18 in-place inspections. On the other hand, the Ombudsman also makes so-called 'remote inspections' by reviewing specific branches data registering activities remotely, that is, without in-place enquiry. In 2007, the total number of remote inspections was 202. As an example of the focus of this kind of inspections it can be pointed out that during 2005, there were 89 remote inspections focusing on human resource management companies and 143 focused on the telecommunications companies.27 Furthermore, the Ombudsman may also start an enquiry on his own initiative. In 2007, there were 14 enquiries commenced on the DPO's own initiative.28

[70]. The reports of the DPO refer to inspections and enquiries initiated by the DPO, which speaks for proactivity in this sphere of activity. Although the number of these cases is relatively low, it may be explained by both the lack of appropriate resources and the concentration on other, preventive, activities.

[27] See, Tietosuojavaltuutetun toimintakertomus *2005*, p. 26 (financial report of the DPO). Available in Finnish at: http://www.tietosuoja.fi/uploads/0gyxd5c8_1.pdf (23.11.2008).

[28] See, Tietosuojavaltuutetun toimintakertomus *2007*, p. 16 (financial report of the DPO). Available in Finnish at: http://www.tietosuoja.fi/uploads/w8a22r.pdf (23.11.2008).

2.5. Monitoring

[71]. According to an interview with the Finnish DPO, the violations of data protection legislation and especially information duties are detected mainly through individual complaints.29 The number of complaints or other sorts of requests for action has been steadily rising during this decade reaching a total number of 930 in 2007.30 Specific statistics are included in Annex 1.

[72]. Although violations are usually detected by individual complaints, also remote inspections have a role at this respect. Stretching on limited branches of government and business activities, they provide a valuable tool for focused investigation of compliance of data protection legislation. However, and lastly, it should be noted that the supervision of duties regarding registration of data processing operations is mainly carried out through notification and permissions procedures. Hence, the majority of the data protection authority's work aims to prevent violations concerning information duties before they occur.

[73]. Because the DPO emphasises preventive and proactive measures, the significance of reactive monitoring has remained fairly limited. However, the actual background of the recent decision of the European Court of Justice in Case C–73/07, Satakunnan Markkinapörssi, may increase the importance of this traditional form of monitoring. The case concerned two companies who collected public data from the Finnish tax authorities in order to publish details of wealth and income of approximately 1.2 million persons in newspapers and through a text-messaging service allowing mobile telephone users to receive information published in the newspaper on their telephone. Following complaints from individuals alleging infringement of their right to privacy, the DPO applied for an order prohibiting Markkinapörssi and Satamedia from carrying on the personal data processing activities at issue. The case was submitted to the Supreme Administrative Court, which referred the case for a preliminary ruling by the Court of Justice on the interpretation of Data Protection Directive.

[74]. Although the judgment of the ECJ leaves it to Supreme Administrative Court,31 to decide whether the activities of the companies have such a journalistic purpose that justifies the limitations to the protection of personal data (see para. 62), it nevertheless makes it evident that the Ombudsman may have and actually sometimes has an active role also in terms of the reactive supervision of data protection legislation.

[29] Interview of Finnish DPO, Mr. Reijo Aarnio at the premises of the DPO 03.11.2008.
[30] See, Tietosuojavaltuutetun toimintakertomus *2007*, p. 25 (financial report of the DPO). Available in Finnish at: http://www.tietosuoja.fi/uploads/w8a22r.pdf (23.11.2008).
[31] As of 19.01.2009, the case is still pending before the Supreme Administrative Court.

2.6. Availability of Decisions

[75]. The decisions of the data protection authorities are available to the public via two web sites. The DPO's website provides a collection of decisions in topically systematised order at http://www.tietosuoja.fi/1554.htm. All the DPB's decisions can be found at http://www.om.fi/1551.htm. They are also available freely on the Finnish legal database Finlex.32 However, no English translations of the decisions are available.

2.7. Relevance of the Opinions of Working Party 29

[76]. The Opinions of the Working Party established under Article 29 of Directive 95/46/EC have been significant especially in terms of the definition of personal data (Opinion Nº 4/2007 on the concept of personal data, WP 136, 20.06.2007) because it clarified the principal concept of data protection rights.33 Otherwise, the opinions of WP29 have been given effect typically in instances where the opinions have been directly relevant for the case at hand. The Finnish DPO considers that the Lisbon Treaty would indirectly increase the significance of the opinions of the working party.

2.8. Advisory Role

[77]. The DPO plays a significant advisory role in Finland. The DPO and the Staff of the Ombudsman's Office are regularly heard in preparation of legislative or administrative reforms concerning the protection of personal rights and freedoms in the processing of personal data. (Administrative reforms refer, for example, to organisational reforms influencing the processing of personal data). During 2007, Parliament heard the DPO in 33 matters (39 in 2006). The total number of statements provided for legislative process of working groups dealing with the preparation and review of legislation was 121 (105 in 2006).34 No information on the concrete effects of the DPO's proposals is readily available. However, nothing indicates that they have not been followed.

[32] See, http://www.finlex.fi/fi/viranomaiset/ftie/ (12.12.2008).

[33] See, Tietosuojavaltuutetun katsaus toimintaan *2007*, p. 8 (annual report of the DPO). Available in Finnish at: http://www.tietosuoja.fi/uploads/w8a22r.pdf (23.11.2008).

[34] See, Tietosuojavaltuutetun toimintakertomus *2007*, p. 8 (financial report of the DPO). Available in Finnish at: http://www.tietosuoja.fi/uploads/w8a22r.pdf (23.11.2008).

2.9. Awareness Raising

[78]. The DPO has played a major role in awareness raising. This has included active participation in public discussions by the DPO, as well as active policy of information dissemination on behalf of the Office of the DPO. The website (www.tietosuoja.fi) for the Office of the DPO is an important channel for providing information on the legislation, decisions and practices in data protection area. The site includes information in multiple languages, including English. Moreover, issued four times a year, the Tietosuoja magazine is published by the Office of the DPO and the DPB and is aimed at controllers in particular. Furthermore, it should also be mentioned that the in-house experts give lectures at seminars arranged both by the Office of the DPO and other organisations. These lectures and seminars are directed towards people responsible for data protection affairs in certain interest groups. Covered sectors include for instance health services, working places and education.35

[35] See, Tietosuojavaltuutetun vuosikertomus *2005*, pp. 11. Available in Finnish at: http://www.tietosuoja.fi/uploads/06tegxehtq.pdf (24.11.2008).

3. Compliance

3.1. Registration of Data Protection Operations

[79]. General framework regarding duties of registration of data processing operations is defined in the Personal Data Act (PDA). According to Section 10, the controller shall draw up a description of the personal data file (rekisteriseloste), indicating in effect the same information that is listed in Article 19(1) (a) to (f) of the Data Protection Directive. The duty of notification is set forth at Section 36 which requires that the controller shall notify the DPO of automated data processing by sending a description of the file to that authority. In addition, the controller shall notify the DPO on certain cases where the personal data is transferred outside the European Union or the European Economic Area or on the launching of an automated decision-making system. Moreover, anyone who is engaged in credit data activity or carrying out debt collection or market or opinion research as a business, or operating in recruitment, personnel assessment or computing on the behalf of another, and who uses or processes files or personal data in this activity, shall notify the same to the DPO. The duty of notification may be derogated in cases listed at Section 36(4).

[80]. Besides general duty to register data processing operations, the PDA does not provide for a particularized duty to log individual processing operations. However, Section 32 provides that the data controller shall carry out the technical and organisational measures necessary for securing personal data against unauthorised access, accidental or unlawful destruction, manipulation, disclosure and transfer as well as against other unlawful processing. Furthermore, Section 33 lays down a secrecy obligation for those who have gained knowledge of someone's personal circumstances. Nevertheless, certain specific legislation requires certain types of processing of personal information to be registered. For instance, Section 5 of the Act on the electric processing of client data within the social and healthcare services (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, Lag om elektronisk behandling av klientuppgifter inom social- och hälsovården, Act no. 159/2007) sets forth an obligation for all the healthcare and social service provides to register all the authorised users of client data as well as to maintain a log for all the instances of processing of client data. Moreover, also Section 13 of the Act on the Status and Rights of Patients authorises the disclosure of the patient data under specific circumstances, but requires that the disclosure as well as reasons for it are recorded to the patient's data file.

[81]. General principles concerning duties of requesting approval of sensitive data processing operations are defined in Personal Data Act. First, although processing of sensitive data is generally prohibited, the PDA authorises it in certain cases defined conclusively at Section 12 of the PDA. Most of the derogations are based on material reasons such as express individual consent and statutory tasks of public authorities. In the scope of application of these derogations, no additional approval is required.

[82]. However, the list also includes a provision (Section 12) concerning processing of data where the DPB has issued a permission, as provided in Section 43, subsection 2. According to Section 43, subsection 2 the DPB may grant permission for the processing of sensitive data, for a reason pertaining to an important public interest. Section 43 further orders that the permission may be granted for a fixed period or for the time being; it shall contain the rules necessary for the protection of the privacy of the data subject. These rules may be amended or supplemented at the request of the DPO or the data subject, if this is necessary owing to a change in circumstances.

3.2. Supervision of Compliance

[83]. The supervision of compliance of both duties regarding registration of data processing operations and duties of requesting approval of sensitive data processing operations are carried out by the DPO and mainly through notification and permissions procedures as well as orders and inspections.

[84]. According to Section 37 of the PDA, the controllers are obliged to make a notification well in advance of the collection or recording of the data to be recorded into the file or of the carrying out of another measure giving rise to the duty of notification and no later than 30 days before the same; hence, the procedure functions as a preventive supervisory mechanism. Similar functions can be associated also to the permissions procedure included in Section 43 in which the DPB may grant permission for the processing of personal data if the processing is necessary, otherwise than in an individual case, in order to protect the vital interests of the data subject, or in order to use the public authority of the controller or a third person to whom the data is to be disclosed. As explained above, the similar procedure also to the processing of sensitive data in specific circumstances.

[85]. These permissions may be granted for a fixed period or for the time being and they must contain the rules necessary for the protection of the privacy of the data subject. The rules may be amended or supplemented at the request of the DPO or the data subject, if this is necessary owing to a change in circumstances. Moreover, at the request of the DPO, the DPB may prohibit processing of personal data which is contrary to the provisions of the PDA or the rules and regulations issued under it. It may also compel the person concerned to remedy

an instance of unlawful conduct or neglect or order that the operations pertaining to the file be ceased, if the unlawful conduct or neglect seriously compromise the protection of the privacy of the data subject or his/her interests or rights, provided that the file is not set up under a statutory scheme. Finally, the permission may be revoked if its prerequisites are no longer fulfilled or the controller acts against the permission or the rules attached to it.

[86]. Inspections by the DPO also aim at assessing compliance with the law of data processing, guiding controllers, improving the standard of systems and preventing violations in advance. The DPO made 10–18 inspections between the years 2002–2007.36

[87]. Also individual complaints concerning access and rectification rights as guaranteed by Sections 28 and 29 of the PDA may have significance in terms of compliance. In fact, a survey conducted by the National Research Institute of Legal Policy in 200637 as well as annual reports of the DPO provide evidence that there are large and widening discrepancies in compliance between private and public sector. While in 1998, the ratio between complaints made by citizens against private and public sector actors was 1:1.17, the same ratio in 2005 was 1:1.74. In other words, the Office of the DPO processed nearly two complaints against a private sector actor for every complaint concerning the public sector. The 2005 review of the DPO suggests the reasons for this are based on the rule of law principle and centralised supervision systems that define the functioning of the public sector whereas the private sector is negatively influenced by the rapid changes in business cultures.38

[88]. Moreover, based on evidence gathered from the DPO's website, as well as jurisprudence from Finnish courts through database Finlex, this compliance is usually achieved through mechanisms that do not rely on the court system. There are hardly any domestic cases regarding particularly the non-compliance of the duties concerning registration of data protection operations. In this respect, the supervisory powers of data protection authorities have displaced the similar role of the courts.

[89]. However, it should also be pointed out that in the recent judgment of the European Court of Human Rights (ECtHR), Finland was found violating Article 8 of the ECHR.39 In this case, health records with information on the claimant's HIV status were apparently available to colleagues in the Finnish

---

36 See, Tietosuojavaltuutetun katsaus toimintaan *2007*, p. 16 (annual report of the DPO). Available in Finnish at: http://www.tietosuoja.fi/uploads/w8a22r.pdf (23.11.2008).

37 See Vesa Muttilainen: Suomalaiset ja henkilötietojen suoja. Kyselytutkimusten ja viranomaistietojen tilastoja 1990-luvulta ja 2000-luvun alusta (Finns and Data Protection. Data based on Surveys and Statistical Data covering the 1990s and early 2000) Helsinki 2006, pp. 50–51. The study is available at: http://www.optula.om.fi/35424.htm, with summary in English at http://www.optula.om.fi/uploads/yg3q4792g4m3d5.pdf (18.11.2008).

38 See, Tietosuojavaltuutetun vuosikertomus *2005*, pp. 3–5. Available in Finnish at: http://www.tietosuoja.fi/uploads/06tegxehtq.pdf (24.11.2008).

39 *I v. Finland* (Application no. 20511/03), Judgment of 17 July 2008.

health clinic she worked in, although records of who had accessed the data were incomplete. The ECtHR held unanimously that there had been a violation of Article 8 on account of the domestic authorities' failure to protect, at the relevant time, the applicant's patient records against unauthorised access.

3.3. Appointment of Data Protection Officers

[90]. Rules on the appointment of data protection officers are still somewhat vague and incomplete in Finland. Specific provisions concerning appointment of data protection officers can only be found from the Act on the Electric Processing of Client Data within the Social- and Healthcare Services as well as from the Act on the Electronic Medical Prescriptions (Laki sähköisestä lääkemääräyksestä, Lag om elektroniska recept, Act no. 61/2007). These Acts require that social and healthcare service providers, and pharmacies, and The Social Insurance Institution of Finland (KELA), and The National Authority for Medicolegal Affairs (TEO) designate Data Protection Officers. However, the formal prerequisites for the officers and their competences are not specified by law.

[91]. The Office of the DPO conducted a survey in 2008 to evaluate how the social and healthcare service providers have addressed privacy and security issues especially in terms of the data protection officers. According to the survey, the providers had not designated a sufficient number of data protection officers. Moreover, the survey demonstrated several shortcomings in the implementation of the statutory obligations regarding protection of patient and social service clients' data. For example, log data monitoring was not adequate nor were the right subjects adequately informed on their right to inspect the registry information and require their repair. Finally, the survey revealed that a number of service providers' responsible leaders did not provide the client and patient data processing personnel with written instructions. The DPO urged the service providers to designate a sufficient number of Data Protection Officers.40 The outcomes of the Ombudsman's suggestion are not yet available.

[40] The results of the survey are available on the website of the DPO at http://www.tietosuoja.fi/44358.htm (23.11.2008).

4. Sanctions, Compensation and Legal Consequences

4.1. Relevance of Sanctions and Compensation Payments

[92]. According to Section 46 of the Personal Data Act (PDA), the DPO may impose a threat of a fine, in accordance with the Act on Threats of a Fine (1113/1990), in order to reinforce the duty to provide access to data and a decision made on the basis of individual complaints concerning access and rectification rights. The DPB may do likewise in relation to the duty to provide access to data and the orders given by the Board at the request of the DPO and on the basis of Section 44 of the PDA. However, these instruments are rarely used. The Ombudsman has requested the Board to impose a threat of fine in three cases during the 2000s. In each of them, this request was dismissed. In one of the cases, the request was dismissed due to the fact that the processing of information was not contrary to the PDA.41 The second case concerned collection of public data from the Finnish tax authorities for the purposes of publishing extracts from the data in the regional editions of the Veropörssi newspaper each year. Hence, it is the same case that was later forwarded to the ECJ for preliminary ruling. The DPB dismissed the request based on arguments stemming from freedom of expression.42 In the third case, the DPO requested that a threat of fine would be imposed against a company which provided so-called fast money loans through mobile networks. The Board ordered the company to change its practices but did not impose a threat of fine. The decision does not give any reason why the request for fines was dismissed.43

[93]. Although existing legislation provides for criminal sanctions relating to data protection violations as well as for compensatory damages, these consequences are uncommon. According to a study published in 2006, criminal offences against the PDA have slightly increased during the present decade, but remain nevertheless at remarkably low levels. For instance, during the year 2004, lower level courts gave only seven decisions on cases like this. In one of them, the charges were dismissed. All the other cases resulted in fines.44 At the same time the police was informed roughly 20 data protection offences and a few data

41 See, Finland/Tietosuojalautakunnan päätös 5/03.09.2003,
42 See, Finland/Tietosuojalautakunnan päätös 1/ 07.01.2004.
43 See, Tietosuojalautakunnan päätös 1/ 22.01.2008.
44 See Vesa Muttilainen: Suomalaiset ja henkilötietojen suoja. Kyselytutkimusten ja viranomaistietojen tilastoja 1990-luvulta ja 2000-luvun alusta. (Finns and Data Protection. Data based on Surveys and Statistical Data covering the 1990s and early 2000) Helsinki 2006, p. 69.

protection violations. Although all misuse is never revealed because of the hidden criminality, there is no doubt the numbers are low compared to other kinds of criminal activity.45

[94]. The hearing procedure included in the PDA (as well as the Penal Code of Finland46) provides additional information on the role of the criminal justice system in the data protection sector. According to Section 41, the public prosecutor shall hear the DPO before bringing charges for conduct contrary to the PDA. Moreover, when hearing a case of this sort, the court shall reserve the DPO an opportunity to be heard. According to the annual report of the DPO, prosecutors and courts made 49 requests for such statements in 2007. In 2006, the number of requests was 46. There has been a significant change in these statistics during this decade. The number of requests increased considerably in 2004 to 50 from 25.47 Complete statistics for the years 2000–2007 are enclosed in Annex 1.

[95]. A recent internal survey, which was conducted by the Office of the DPO, used the hearing procedure provided by both the Penal Code and Section 41 of the PDA as a source of its baseline data.48 The survey analysed the legal consequences of those cases where police, prosecutor or a court had requested the statement of the DPO during 2007. By December 2008, the District Courts (general courts of the first instance) had already decided 20 of these cases. In 17 cases, the judgments are final.

[96]. During the period of survey, the District Courts gave 12 sentences for data protection offences, four sentences for secrecy offences, three sentences for computer break-in, two sentences for defamation, two sentences for violation of official duty, one sentence for invasion of private reputation, and one sentence for secrecy offence. Illustrative of the current state of legal practices is the case in which the Tuusula District Court argued that charges concerning data protection offences are "so rare that no consistent sentencing practice exist as of yet".

[97]. This statement of the Tuusula District Court is in line with the similar findings of this report. Notwithstanding the increase in requests of statements from the DPO by the courts and prosecutors, there remains the lack of extensive case law

45 See Vesa Muttilainen: Suomalaiset ja henkilötietojen suoja. Kyselytutkimusten ja viranomaistietojen tilastoja 1990-luvulta ja 2000-luvun alusta. (Finns and Data Protection. Data based on Surveys and Statistical Data covering the 1990s and early 2000). Helsinki 2006, pp. 66–68.

46 See, Chapter 38, Section 10, subsection 3 of the Penal Code (*Rikoslaki, Strafflag*, 39/1889) Unofficial English translation available at http://www.finlex.fi/fi/laki/kaannokset/1889/en18890039.pdf (22.12.2008).

47 Statistics for the years between 2002 and 2007 are included in Finland /Tietosuojavaltuutetun toimintakertomus *2007*, p. 19. (2007 financial report of the DPO). Available in Finnish at: http://www.tietosuoja.fi/uploads/w8a22r.pdf (23.11.2008).

48 See, Tiia Poroila: Rangaistuskäytäntö tietosuojarikoksissa (Sentencing Practice in Data Protection Crimes). Internal Memo Prepared for the DPO's Office. December 2008. On file with the authors.

on data protection crimes. The reason for the limited number of criminal cases dealing with data protection issues might stem partly from the fact that personal data is not widely misused in a manner that would wake up criminal concerns. This may of course relate to both lack of awareness and lack of actual criminal practices. Moreover, lack of clear jurisprudence from courts may heighten the threshold for reporting offences. In fact, the DPO stated in the interview that there seems to be a lack of awareness among courts and prosecutors on their statutory duty to hear the DPO in their cases involving charges for conduct contrary to the PDA.

[98]. Finally, although the DPO possesses the authority to report unlawful conduct for prosecution, these cases have also remained rare. According to statistics, the Ombudsman reported unlawful conduct for criminal investigation in ten cases between 2000 and 2007.49

[99]. No systematic studies and hence objective information regarding proof of intent or negligence in data protection cases is available. However, there are no reasons to suspect that standard principles of criminal process, which include the principles of favor defensionis and in dubio pro reo were not applied in these cases.

[100]. In terms of compensatory payments, the basic provisions are included in the Tort Liability Act (Vahingonkorvauslaki, Skadeståndslag, Act no. 412/1974). Moreover, the PDA enacts specifically that the controller is liable to compensate for the economic and other loss suffered by the data subject or another person because of processing of personal data in violation of the provisions of the PDA.

[101]. Even though no systematic research is available about compensatory damages awarded for data protection violations, the existing court practice suggests these cases are extremely rare. There is no case law by the Supreme Court solely on this issue. However, one Supreme Court Decision, Finland/Korkein oikeus/KKO 2005:136 (19.12.2005), provides for an analogous example.50 In that case, a magazine had published a report of a violent offence of which X had been committed. The question was whether disclosing X's name in the report was a violation of his privacy in the meaning of Chapter 5, Section 6 of the Tort Liability Act which provided for right to damages also for the anguish arising from an offence against liberty, honour or the domestic peace or from another comparable offence. After weighing the defendant's freedom of expression against X's privacy rights, the Supreme Court concluded that X's privacy rights were not violated in a manner that would have caused personal damage to X in the meaning of the Tort Liability Act. Three dissenting justices of the Supreme Court held that because of the exceptionally grave nature of X's offence, it was

[49] There were one report to police in 2003, two in 2004 and seven in 2005. Information is based on e-mail conversation with Elisa Kumpula, the Head of Department of the Data Protection Ombudman's Office o4.12.2008 (on file with the authors).

[50] The case is available in Finnish at http://www.kko.fi/34046.htm (01.12.2008).

undisputable that informing the public of the offence contributed to a debate of general interest in society. However, considering the nature and content of the report, which was based on an interview with the victim, telling the offender's name was not necessary and did not contribute to the public debate. The dissenting justices concluded that X was entitled to compensation because of an invasion of his privacy.

[102]. The Supreme Court's decision implies the difficulties relating to the possibilities of receiving damages based on violation of data protection rights which are heightened by the fact that the plaintiff carries both the burden of proof and the risk for legal costs. The relative insignificance of both compensatory damages and criminal justice system in data protection issues may also be explained by significance of data protection authorities. For example, the number of individual complaints and requests for guidance submitted to the DPO by the individuals has more than doubled during the last ten years, reaching 840 cases in 2004, 868 cases in 2005 and 939 cases in 2006.51 As the data protection authorities are not authorised to award damages or to order direct sanctions, these consequences remain dependent upon further court proceedings in the ordinary court system. Yet, the interest to pursuit these legal consequences is reduced because of the fact that the powers that the data protection authorities are entrusted with usually suffice to resolve the data protection issue at hand.

[103]. Hence, sanctions and compensation payments do not represent significant mechanism for enforcement of data protection legislation in Finland. To condense, this state of the matters is a result of various reasons. First, the system of data protection, as it currently stands, relies heavily on preventive measures. In fact, the Finnish DPO views every court case as an instance of failure to fulfil his primary aim, which is the prevention of data protection violations.52

[104]. Second, and in terms of damage payments, although the possibility to receive legal aid by those who cannot afford the necessary assistance reduces the risk in some cases, the ultimate financial risk of litigation is carried by the individual seeking for compensation. Third, data protection authorities seem to provide adequate protection for the realisation of rights in a way that mitigates the urgency of other forms of legal consequences, such as criminal sanctions as well as compensatory payments. And fourth, lack of case law, hence information regarding appropriate scope of compensatory damages in data protection issues may itself reduce the bringing of new cases to the court system.

[105]. Enforcement of data protection legislation through sanctions and/or compensation payments does not depend largely on personal initiative of data

[51] See, the Annual Report of the DPO 2005, p. 59. Available in Finnish at: http://www.tietosuoja.fi/uploads/06tegxehtq.pdf (24.11.2008), and the Annual Report of the DPO 2006, p. 72. Available in Finnish at: http://www.tietosuoja.fi/uploads/u5a147mca.pdf (24.11.2008).

[52] Interview with the Finnish DPO Mr. Reijo Aarnio 03.12.2008.

subjects. This is due to the emphasis on preventive official mechanisms as well as the fact that sanctions and compensation payments simply do not represent significant mechanism for enforcement of data protection legislation in Finland.

4.2. Follow-up Activities

[106]. The follow up activities do not represent individually reported and in that sense a significant part of practices of data protection authorities in Finland. In fact, the office of the Ombudsman, to whom these functions would belong, emphasises strongly the preventive measures as their primary duties. For instance, the DPO's annual report 2006 presents it as a merit that the Ombudsman's office concentrates heavily on preventive measures resulting to such division of labour, where only one-fifth of work hours are allocated to the processing of individual complaints.53 Moreover, the annual reports of the DPO do not include detailed information about follow-up activities although they list and explain the most important cases decided during the year under report. Clear statistical information about the consequences of Ombudsman's activities is also lacking. However, it is reasonable to presume that part of the activities of the DPO serve also follow-up purposes. These include self-initiated inspections and other sorts of enquiries. Nevertheless, there clearly does not exist any clear policy to support systematic follow-up activities.

4.3. Personal Data Collected and Processed in the Context of Employment

[107]. The protection of personal data collected and processed in the context of employment is mainly provided by the Act on the Protection of Privacy in Working Life (Laki yksityisyyden suojasta työelämässä, Lag om integritetsskydd i arbetslivet, Act no. 759/2004). However, the Act on the Protection of Privacy in Electronic Communications also lays down important rules regarding the sphere of privacy in the context of employment.

[108]. According to Section 3, subsection 1 of the Act on the Protection of Privacy in Working Life, the employer is only allowed to process personal data directly necessary for the employee’s employment relationship which is connected with managing the rights and obligations of the parties to the relationship or with the benefits provided by the employer for the employee or which arises from the special nature of the work concerned. Subsection 2 of Section 3 provides that no exceptions can be made to the necessity requirement, even with the employee’s consent.

53 See, Annual Report of the DPO 2006, p. 7. Available in Finnish at: http://www.tietosuoja.fi/uploads/u5a147mca.pdf (24.11.2008).

[109]. Section 4 of the above-mentioned law sets forth the general requirements for collecting personal data about employees and the employer's duty to provide information. The employer shall collect personal data about the employee primarily from the employee him/herself. In order to collect personal data from elsewhere, the employer must obtain the consent of the employee. However, this consent is not required when an authority discloses information to the employer to enable the latter to fulfil a statutory duty or when the employer acquires personal credit data or information from the criminal record in order to establish the employee's reliability.

[110]. Moreover, the employer must notify the employee in advance that data on the latter is to be collected in order to establish his/her reliability. If information concerning the employee has been collected from a source other than the employee him/herself, the employer must notify the employee of this information before it is used in making decisions concerning the employee. The employer's duty to provide information and the employee's right to check the personal data concerning him/herself are also subject to other relevant provisions of the law.

[111]. The role of the unions as well as works councils in terms of the compliance monitoring is based on the cooperative procedure referred to in the Act on Cooperation within Undertakings (Laki yhteistoiminnasta yrityksissä, Lag om samarbete inom företag, Act no. 725/1978) and the Act on Cooperation in Government Departments and Agencies (Laki yhteistoiminnasta valtion virastoissa ja laitoksissa, Lag om samarbete inom statens ämbetsverk och inrättningar, Act no. 651/1988) which provide the general mechanisms in promoting interaction between the management and the staff, and among members of the staff. According to Section 4, subsection 3 of the Act on the Protection of Privacy in Working Life, the collection of personal data during recruitment and during an employment relationship is governed by these Acts on cooperative procedures. The same procedure is applied also to the cases involving camera surveillance (Section 17) and organising technical monitoring and data network use (Section 21).

[112]. Even though the system of protection of privacy in the work places has been relatively well developed in Finland, the Government Bill concerning the amendment of the Act on the Protection of Privacy in Electronic Communications as well as some other laws54 seems to put the whole system in quite a troublesome shade. The amendment, which is currently pending before Parliament, would give companies the right to monitor the addresses of e-mails sent and received by employees, as well as the type of attachments linked with the message, but not the content of the message itself. According to the Bill, companies will be given a right to process identification data in their communications networks to detect, prevent and investigate violations of business secrets, unauthorised use, espionage as well as certain other crimes.

[54] See, Government Bill HE 48/2008 vp.

These kind of snooping rights have been argued to be especially important for the mobile telephone manufacturer Nokia. In fact, Nokia has been investigated several times for suspicions concerning violations of the law on data protection of electronic communications.55 Moreover, several employees, including Company's CEO, of the largest telecom operator of Finland, Sonera have been convicted for similar violations.56 The amendment to the Act on the Protection of Privacy in Electronic Communications would practically legalise significant part of the kind of measures that have so far been under criminal investigations.

[113]. As noted by the constitutional law experts during the earlier phases of the legislative process, the Government Bill was highly problematic from a constitutional perspective for being motivated purely by the economic interests and their protection which were given a clear advantage over the protection of privacy. However, in its recent opinion, heavily criticised both by constitutional experts and the media,57 the Constitutional Law Committee of Parliament approved the bill.58 According to the Committee's opinion, the amendment was not unconstitutional although it would allow employers to investigate the log data of employees' e-mails, if the company has reason to suspect that corporate secrets are leaking out of the company or that the employer's communication networks are being misused. This was held to be allowed by the Constitution because the rights of the employer would not cover the inspection of the content of the messages themselves, but only authorised them to examine the e-mail log including the information on the senders, the recipients, and the size of employee messages as well as the volume of traffic and other matters relating to the company's e-mail usage. Moreover, the Committee stressed that a company can be allowed to investigate the e-mail log only after it has taken all other legal measures to prevent potential wrongdoing.

[114]. In spite of these delimitations, major problems remained. For instance, as argued by one of the experts heard by the Constitutional Law Committee, professor Veli-Pekka Viljanen of the University of Turku, 'the core problem is

55 For instance, the international edition of the largest newspaper in Finland, *Helsingin Sanomat* has published two independent articles on the issues. See, ' Nokia snooped on employee e-mail communications in 2005', published 09.06.2008, available at http://www.hs.fi/english/article/Nokia+snooped+on+employee+e-mail+communications+in+2005/1135237031018 (01.12.2008) and 'Prosecutor: Nokia dug up e-mails in effort to plug information leaks in 2000–2001', published 18.04.2006, available at http://www.hs.fi/english/article/Prosecutor+Nokia+dug+up+e-mails+in+effort+to+plug+information+leaks+in+2000-2001/1135219561241 (01.12.2008).

56 See, 'Five get suspended sentences in Sonera telephone record case', published in the international edition of *Helsingin Sanomat* 30.05.2005, available at http://www.hs.fi/english/article/Five+get+suspended+sentences+in+Sonera+telephone+record+case/1101979719153 (1.12.2008) and 'Court of Appeals affirms sentences in Sonera snooping case', published in the international edition of *Helsingin Sanomat* 16.03.2007 (01.12.2008).

57 See, for instance 'Legal experts say "Lex Nokia" violates constitution', published in the international edition of *Helsingin Sanomat* 14.11.2008, available at http://www.hs.fi/english/article/Legal+experts+say+%E2%80%9CLex+Nokia%E2%80%9D+violates+constitution/1135241264898 (01.12.2008).

58 See, PeVL 29/2008 vp.

that the employer would decide when corporate secrets are involved, and what constitutes a well-founded reason to suspect a leak of information. The authority of an employer would simply be too broad. It is also problematic that an employer would not have to get any authorisation from anyone, as officials do'.59

[59] See, 'Experts say "Lex Nokia" violates constitution', published in the international edition of *Helsingin Sanomat* 14.11.2008, available at http://www.hs.fi/english/article/Legal+experts+say+%E2%80%9CLex+Nokia%E2%80%9D+violates+constitution/1135241264898 (01.12.2008).

5. Rights Awareness

[115]. The awareness of data protection issues has been studied in two large surveys in Finland. In 2006, the National Research Institute of Legal Policy published a study that surveyed the attitudes and views of the Finnish citizens on data protection issues covering a time period between 1990s and 2004.60 The study was based on population surveys and data provided by public authorities, including Statistics Finland's study on the information society, and the activities of the DPO, decisions issued by the DPB, as well as offences violating the provisions of the Personal Data Act.

[116]. The study reaches several conclusions. First, compared to other EU countries, a somewhat smaller proportion of the Finnish population was, in 2003, suspicious of their personal data protection. Every second Finn over 15 years of age was concerned about their privacy in relation to the processing of their personal data. One reason for this can be assumed to lay in the fact that approximately two Finns out of three consider information on data protection issues to be sufficiently available. Hence, the group holding an opposite view is nonetheless fairly large. The study argues that increased information is one way of enhancing citizens' awareness, improving thereby the status notably of the more passive population groups.

[117]. The study also reveals that every third Finn considers that he or she has had to give too much information about him- or herself to the registers of authorities and enterprises. In addition to this, one out of eight has observed faults in their own register data and seven per cent have requested a clarification about them by the controller. As evidence of growing rights awareness, the number of cases brought by citizens to the attention of the Office of the DPO has doubled in ten years. In 2004, there were some 2,000 written communications addressed to the Ombudsman, out of which citizens initiated 840. As an interesting observation concerning the rights awareness vis-à-vis citizens attitudes toward the state, the study pointed out that the most cases involving the right to verify data and their rectification concerned sectors where citizens are least suspicious (health care, police), according to Finnish surveys. It can be assumed that cases in these sectors most commonly involve disputed issues that are important at a level of principle, to which the data subjects want the DPO to take a stance.

[118]. Finally, according to the National Research Institute of Legal Policy's survey, the problems citizens encounter concerning data protection involve a great variety of actors in the public as well as private sectors. A fairly even share of respondents considered they had given too much information both to authorities

[60] See Vesa Muttilainen: Suomalaiset ja henkilötietojen suoja. Kyselytutkimusten ja viranomaistietojen tilastoja 1990-luvulta ja 2000-luvun alusta. OPTL:n julkaisuja 218. Helsinki 2006. The study is available at: http://www.optula.om.fi/35424.htm, with summary in English at http://www.optula.om.fi/uploads/yg3q4792g4m3d5.pdf (18.11.2008).

and to enterprises, but public registers are checked to a higher degree than those of enterprises. There were also an equal number of persons, who had found errors in their personal data in registers of both authorities and enterprises. Nevertheless, criminal offences against the Personal Data Act are still rare, although there has been a certain increase in their number during the present decade.

[119]. The second large survey, which was ccommissioned by the Ministry of Employment and the Economy, concentrated on the issues relating to privacy and data protection at the workplaces.61 The survey was carried out by using sociological and legal methods. The empirical material was based on postal questionnaire that was sent to a sample of 1,296 enterprises and public offices. The return rate was 35 per cent.

[120]. According to empirical study, the respondents were quite well aware of the data protection legislation. More than 90 per cent of the workplaces had an email system and/or internet. Four out of five respondents did not see any data protection issues relating to uses of e-mail and internet. However, five per cent of surveyed announced suspicions of privacy breach and one per cent of the respondents declared to be victims of concrete case of violations of their right to confidentiality of correspondence.

[121]. The survey also analysed other data protection related issues such as video monitoring and drug testing. Video monitoring was used in more than 2/3 of the state offices and private firms. Instead, somewhat less than a half of the municipal bureaus have used it. However, more than ten per cent among the respondents of the employees said that there had been no negotiations about monitoring at the workplace.

[122]. The above-mentioned surveys did not analyse the role of NGOs in terms of rights' awareness. Two distinct organisations should be mentioned in this respect. The first, Electronic Frontier Finland association (Effi), was founded in 2001 to 'defend active users and citizens of the Finnish society in the electronic frontier'. Effi influences legislative proposals concerning, e.g., personal privacy, freedom of speech and user rights in copyright law. It makes statements, press releases and participates actively in actual public policy and legal discussion. The second, recently established Piraattipuolue (Pirate Party), mainly strives to reform laws regarding intellectual property, including copyright and patent laws. However, their agenda also includes support for a strengthening of the right to privacy, both on the internet and in everyday life.

[61] Kuokkanen, Taina - Laitinen, Ahti - Kairinen, Martti: Työelämän yksityisyyden suoja – Tutkimus päihteiden käyttötietojen ja kameravalvonnan sekä sähköpostiviestien suojasta. Työ- ja elinkeinoministeriön julkaisuja.Työ ja yrittäjyys. 10/2008. Edita Publishing 2008. The study is available at: http://www.tem.fi/files/19052/temjul_10_2008_tyo_yrittajyys.pdf, with summary in English at p. 150. (18.11.2008).

6. Analysis of deficiencies

[123]. Although the Finnish system of data protection works relatively well from the perspective of fundamental rights, certain deficiencies should be pointed out.

[124]. First, the constitutional standards involving protection of personal data are somewhat underdeveloped in Finnish constitutional jurisprudence. The Constitutional Law Committee of Parliament has not managed to construe a coherent doctrine that would be vital for the effective protection of these rights in legislative as well as in administrative and judicial practices. Instead, the Committee adheres to several different standards, which leads to reduced certainty of the right in question. Especially troublesome development in this respect concerns the recent opinion of the Committee on the amendment to the Act on the Protection of Privacy in Electronic Communications.62

[125]. As explained above, the amendment, which the Committee held to be constitutional, gives the employer and the internet service provider wide processing rights to identification data in their communications networks. Although the exercising of these rights is limited to the cases and extent where the processing is necessary for the purpose of reporting the offence to the police, it is crucial to understand, that these rights may be exercised independently, hence without authorisation from a court or a public authority. To emphasize: under the Coercive Measures Act (Pakkokeinolaki, Tvångsmedelslag, Act no. 450/1987), the police needs a court's permission to use log data which may be granted if the maximum punishment for a suspected crime is at least four years imprisonment. In contrast, according to the amendment to the Act on the Protection of Privacy in Electronic Communication, the authorisations to investigate private communications by a private organisation neither require a court order nor are they connected to compelling interests relating to investigation of serious offences. The maximum sentence for violating corporate secrecy is two years imprisonment.

[126]. It is fair to claim, that with its opinion, the Committee practically discards the firm position it had held earlier regarding the legislatures' constitutional duty to adopt measures designed to secure respect for private life and personal data also in relations that individuals have between themselves. Instead, it employs a new doctrine effectively diminishing a large part of the constitutional protections of personal data in relations between private parties. In this sense, it has created a troublesome precedence for all the future cases relating to protection of personal data and privacy in the private sphere.

[127]. Second, the Finnish system of data protections relies heavily on preventive and legally somewhat soft methods of supervision like for instance guidance. There

62 See, PeVL 29/2008 vp.

is no doubt that these methods of securing the compliance ex ante must be preferred to those ex post facto guarantees that are provided by the criminal justice system. Moreover, in terms of the effective realisation of rights, preventive mechanisms serve this end better than for instance individual court proceedings or other sorts of reactive measures.

[128]. However, overt concentration on the preventive instruments can lead to unbalance where already occurred abuses of rights are left without appropriate legal treatment. Although the current Finnish practices do not represent a major problem at this respect, two main deficits can nevertheless be pointed out. First, the Finnish data protection authorities seem to lack orderly follow-up procedures for the instances of noncompliance they discover during their ordinary activities. This is illustrated already by the fact that the annual reports of the DPO provide accurate statistical information about the number of the cases they have dealt with during the reporting year but no information about the content and consequences of Ombudsman's decisions in concrete cases. Second, the present Finnish system effectively rules out the factual possibilities to seek for compensation for the violation of a data protection rights. This is due to the combination of several factors such as burden of proof, difficulties relating to quantification of the damage as well as the fact that the decisions of data protection authorities, although not being able to provide monetary compensation, nevertheless are usually able to correct the original instance of violation. Although better possibilities to receive monetary compensation would hardly alone provide sufficient guarantees for data protection, they would most certainly enhance both the fairness of the system as a whole and the active implementation of the rights guaranteed already by the Constitution. One can at least assume that the higher the risk of being ordered to pay compensation for the noncompliance of data protection obligations, the greater the probability that those obligations are respected in future cases.

[129]. Third, the legislation concerning data protection is widely dispersed to different sector-specific enactments. This has caused the legislation to be both inconsistent and complex. Moreover, also the supervision of data protection is dispersed to several public authorities as not only the data protection authorities but also the Finnish Communications Regulatory Authority, and the ministries of Justice, Traffic and Telecommunications and Labour have separate powers in this sphere. Because of the inconsistencies as well as overlaps between different departments of law, respective legislation, and authorities unexpected gaps of protection may arise in concrete practices.

[130]. For instance, in one case decided by the Administrative Court of Kuopio, the Trade Register Act (Kaupparekisterilaki, Handelsregisterlag, Act no 129/1979) was argued to override the rectification rights provided by the PDA. The case was brought to the Administrative Court by the National Board of Patents and Registration after the DPO had issued it with an order to remove erroneous information from the trade register. According to the Trade Register Act, rectification could be made only after a court order whereas the PDA obligated

the controller to rectify, erase or supplement personal data contained in its personal data file on its own initiative or at the request of the data subject, or on order of the DPO. The Administrative Court dismissed the appeal of the National Board of Patents and Registration by referring to the constitutional and international background of the PDA and holding that for this reason, the PDA overrides the Trade Register Act.

[131]. The case illustrates the problems relating to overlapping legislation. However, as explained above, there also exists certain lack of knowledge among courts and prosecutors even in the cases where the law is clear. Moreover, the level of protection of personal data in private sector has declined quite significantly during the last years. Although no systematic research is available for the reason of these tendencies, the current state of the legislation contributing to a fairly complex and fragmentary system of data protection seems to provide at least one candidate.

[132]. There are a number of routes available for filling these deficiencies. Problems in the interpretation of the constitutional guarantees of data protection need to be managed on that level, namely by developing coherent standards of interpretation. Second, the current functioning of the supervision of data protection legislation that emphasises preventive and mainly administrative and managerial measures needs to be supplemented with systematically employed subsequent mechanisms that include a realistic possibility to receive damages for misuses of personal data. Naturally, also appropriate resource allocations are needed for achieving this end.

[133]. The lack of actual and efficient remedies is partly a larger problem in the Finnish system of fundamental rights protection. As for instance the Parliamentary Ombudsman pointed out in her Annual Report of 2005, the Finnish system as presently constituted does not provide an effective and comprehensive legal remedy in the form of redress for a violation of a fundamental right. She emphasised a need for official strategy on the issue, which would cover all sectors of administration and be aimed at protecting human rights.63

[134]. Finally, the complexity of the current data protection legislation cannot be without significance in terms of both the conduct of the public and private controllers and the awareness of the public. It appears that the current legislation has opted for casuistic and sector-specific legislation and codes of conduct instead of purporting to articulate a fairly precise set of general principles applicable in all fields of law. In this particular sense, the deficiencies are caused simultaneously by both domestic and EU legislation.

63 See Eduskunnan oikeusasiamiehen kertomus vuodelta *2005*,
English summary of the Annual Report of Parliamentary Ombudsman 2005, p. 10. available at
http://www.oikeusasiamies.fi/dman/Document.phx/eoa/english/annualreports/2005en?folderId=eoa%2Fenglish%2Fannualreports&cmd=download (28.11.2008).

7. Good practices

[135]. The good practices involving effective data protection measures and relevant institutions in Finland emerge from three main sources.

[136]. First, protection of personal data is explicitly enumerated as part of Section 10 of the Constitution, which protects the right to private life and confidential communications. Hence, there is no need for construing the argument about the validity of personal data protection as a derivative right provided by a more general right to privacy as it is necessary for instance in the context of the European Convention on Human Rights.64 Due to the fact that the issue has already been settled in the wording of the Constitution, the personal data protection issues have a clear and fixed constitutional standing from the outset. Moreover, because international human rights obligations binding upon Finland are understood to provide a minimum standard of protection for the equivalent rights under the Constitution of Finland and because the Constitution requires public authorities to provide a higher or more extensive protection to various rights under the Constitution of Finland, the constitutional status of data protection means also that it ought to be better protected compared to available international standards.

[137]. Second and interlinked with the above-mentioned feature, the explicated purposes of the existing legislation as well as the standards used for its interpretation are conscientiously tied to fundamental rights and international human rights in general as well as to privacy rights in particular. Although this aim does not always concretise in legal or legislative practices, it nevertheless creates a principled foundation for the data protection measures and the respective institutions through which the concrete practices can be evaluated and developed. Moreover, when used actively, the same foundation can be used for a coherent basis for wide ranging data protection policies.

[138]. And third, data protection authorities and especially the Finnish DPO have embraced particularly wide approach to proactive measures obtainable for the development and supervision of data protection legislation. For the most part, this kind of approach is already required by the existing law. Section 40 of the PDA requires the DPO to promote good processing practice and issue directions and guidelines so as to achieve a situation where unlawful conduct is not continued or repeated and to issue more detailed guidelines on how personal data is to be secured against unlawful processing. However, the current Office of the DPO has taken these obligations particularly seriously.

[139]. For instance, the DPO and the personnel of his office are regularly heard in the preparatory work of virtually all new data protection legislation. In fact, the

64 See, *Copland v. the United Kingdom*, paras. 43–44 (Application no. 62617/00, Judgment of 3 April 2007).

DPO must be heard in matters of preparation of legislative or administrative reforms concerning the protection of personal rights and freedoms in the processing of personal data. (Administrative reforms refer, for example, to organisational reforms influencing the processing of personal data). In practice, this means that the Ombudsman provides statements and participates in working groups set up for the preparation and review of legislation. The prerequisites of processing personal data must be taken into account as early as possible in the course of the preparation. The public prosecutor must consult the DPO prior to bringing charges based on violations of the PDA. Courts of law are also obliged to provide the Ombudsman with an opportunity to be heard in cases concerning related issues.

[140]. As the primary duty of the DPO is to influence, in advance, compliance with the legislation concerning the keeping of registers, the Office of the Ombudsman provides information on the PDA, aimed at both controllers and data subjects. As instances of good practices in this respect, it should be mentioned that the in-house experts give lectures to the members of interest groups in the area of data protection at seminars arranged both by the Office of the DPO and other organisations. Issued four times a year, the Tietosuoja magazine is published by the Office of the DPO and the DPB and is aimed at controllers in particular. Moreover, advice is also given by telephone. The guidance and consultation relating to various data system projects is a task field which is important and constantly growing. And finally, the website (www.tietosuoja.fi) of the Office of the DPO is another important channel for providing information in multiple languages.

[141]. And finally, the PDA emphasises the self-steering of register keeping. Controllers and communities representing them can compile field-specific Codes of Conduct for the application of the Act and for promoting good data processing practices. The DPO provides guidance and consultation in the compilation and review of the Codes of Conduct.

Annexes

Annex 1 – Tables and Statistics

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority (DPO)	1050	1116	1287	1250	1266	1298	1376	1492
Staff of data protection authority (DPO's office)	18	19	19	19	20	20	19	20
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	14	19	26	20	27	20	33	14
Number of data protection registrations	116	122	731	478	178	179	225	184

Number of data protection approval procedures (DPB)	11	6	9	10	7	6	7	7
Number of complaints/requests for action received by data protection authority (DPO) (disaggregated below)	577	707	793	752	726	868	939	901
• Concerning supervision of legality	n/a	n/a	n/a	n/a	158	193	275	224
• Concerning guidance	n/a	n/a	n/a	n/a	568	675	664	677
Number of complaints upheld by data protection authority	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

issued, sanction issued etc.)								
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)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Other available statistics

Supervision of Compliance	2000	2001	2002	2003	2004	2005	2006	2007
Requests of statements received by the DPO from the Courts and Prosecutors (relating to cases concerning violations of Personal Data Act)	20	9	17	25	50	41	44	49

Number of matters referred to the police by the Data Protection Authority	-	-	-	1	2	7	-	-
Number of matters referred to the DPB by the DPO	-	-	-	2	-	-	-	1
Decisions of the DPB (permissions and orders)	11	5	7	9	6	6	4	6
• Application Upheld	6	2	6	5	4	5	3	3
• Application dismissed	5	3	1	4	2	1	1	3
• Application Withdrawn	-	1	2	-	-	-	-	-

Advisory Role of the DPO	2000	2001	2002	2003	2004	2005	2006	2007
Requests of statements received by the DPO from the Courts and Prosecutors (relating to cases concerning violations of Personal Data Act)	20	9	17	25	50	41	44	49
Statements on legislative reforms	26	31	30	21	38	45	39	43
Parliamentary hearings	22	19	23	13	22	29	39	33
Statements on administrative reforms	23	23	19	15	21	20	33	37
Statements on International norms and treaties	5	4	13	7	5	11	7	8

Total number of Statements in Advisory role	76	77	85	56	96	105	118	121

Inspections and enquiries	2000	2001	2002	2003	2004	2005	2006	2007
Inspections	11	25	16	15	13	17	10	18
Remote Inspections	n/a	9	9	35	172	254	69	202
• Branch based	n/a	n/a	n/a	n/a	69	232	69	200
• Internet Police Survey	n/a	n/a	n/a	28	101	22	-	-
• DIY Inspections	n/a	9	9	7	2	-	-	2
Self-initiated Enquiries	14	19	26	20	27	20	33	14

Schengen	n/a	n/a	n/a	n/a	1	1	1	1
Nordic Inspections	n/a	n/a	n/a	n/a	3	-	-	-
Total number of Inspections (investigations, audits etc.) conducted by the DPO	25	53	51	70	216	292	113	237

Annex 2 – Case Law

Case title	C‑73/07, Tietosuojavaltuutettu v Satakunnan markkinapörssi and others
Decision date	16.12.2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	C-73/07 The Court of Justice of the European Communities
Key facts of the case (max. 500 chars)	For several years, the company Markkinapörssi has collected public data from the Finnish tax authorities for the purposes of publishing extracts from those data in the regional editions of the Veropörssi newspaper each year. The information contained in those publications comprises the surname and given name of approximately 1.2 million persons whose income exceeds certain thresholds as well as the amount. Markkinopörssi and Satamedia, an associated company to which the data at issue were transferred in the form of CD-ROM discs, signed an agreement with a mobile telephony company which put in place, on Satamedia's behalf, a text-messaging service allowing mobile telephone users to receive information published in the Veropörssi newspaper on their telephone for a charge. On request, the personal data are removed from that service. Following complaints from individuals alleging infringement of their right to privacy, the DPO applied for an order prohibiting Markkinapörssi and Satamedia from carrying on the personal data processing activities at issue. The Supreme Administrative Courta sked the Court of Justice to rule on the correct interpretation of The Data Protection Directive. It wished to know in particular in what circumstances the activities in question can be considered as data processing undertaken solely for journalistic purposes and may, accordingly, be the subject of

	derogations and limitations relating to data protection.
Main reasoning/argumentation (max. 500 chars)	According to the court, Member States should, while permitting the free flow of personal data, protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy, with respect to the processing of those data. In order to reconcile the protection of privacy and the right to freedom of expression, the Member States are require to provide for a number of derogations or limitations in relation to the protection of data and, therefore, in relation to the fundamental right to privacy. Those derogations must be made solely for journalistic purposes or for the purposes of artistic or literary expression, which fall within the scope of the fundamental right to freedom expression, in so far as it is apparent that they are necessary in order to reconcile the right to privacy with the rules governing freedom of expression.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Court of Justice held that the activities of Markkinapörssi and Satamedia constitute data processing within the meaning of the Data Protection Directive even though the files of the public authorities that are used comprise only information that has already been published in the media. Were the position to be otherwise, the directive would be largely deprived of its effect. It would be sufficient for the Member States to publish data in order for those data to cease to enjoy the protection afforded by the directive.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The court considers that activities such as those carried on by Markkinapörssi and Satamedia and which concern data from documents which are in the public domain under national legislation may be classified as 'journalistic activities' if their object is the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them. They are not limited to media undertakings and may be undertaken for profit-making purposes. It is for the Supreme Administrative Court to determine whether the activities at issue in the main proceedings have as their sole object the disclosure to the public of information, opinions or ideas.

Proposal of key words for data base	Personal data, freedom of expression, income-tax publicity, commercial services.

Case title	KKO 2005:136
Decision date	19.12.2005
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	KKO 2005:136; Diaarinumero: S2003/534 Esittelypäivä: 28.09.2005 Antopäivä: 19.12.2005 Korkein oikeus [Supreme Court]
Key facts of the case (max. 500 chars)	A magazine had published a report of a violent offence of which X had been convicted. The question was whether disclosing X's name in the report was a violation of his privacy in the meaning of Chapter 5, Section 6 of the Tort Liability Act which provided for right to damages also for the anguish arising from an offence against liberty, honour or the domestic peace or from another comparable offence.
Main reasoning/argumentation (max. 500 chars)	The Supreme Court held that disclosing the name or identity of an offender in the media without the person's consent always constitutes some kind of intrusion in the person's private life. On the other hand, there may be circumstances that speak in favour of the right of the public to be informed of the name and identity of the offender. In this case, X had been convicted of an exceptionally grave assault involving deeds, which degraded the victim and his dignity. The majority of the Court held that in case of grave offences, which attract the public's attention, the identity of the offender tends to be revealed eventually one way or another. This is a consequence of the offence and X should also have been prepared for it. The Court also pointed out that the report had been published shortly after the trial, and was thus a topical piece of news at that time. The tone in the report was factual. Apart from X's name, his photo or other information pertaining to his private life had not been published. Three dissenting justices of the Supreme Court made a clearer distinction between the offender and his acts. They held that because of the exceptionally grave nature of X's offence, it was undisputable that informing the public of the offence contributed to a debate of general interest in

	society. However, considering the nature and content of the report, which was based on an interview with the victim, telling the offender's name was not necessary and did not contribute to the public debate.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The case concerns to right of the media to disclose the name and identity of an offender without person's consent. According to the majority of the court, the name can be disclosed even though the disclosure as such would not contribute to the public debate. Instead, the crime as such, in cases of grave offences, also justifies the disclosure.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	After weighing defendant's freedom of expression against X's privacy rights, the Supreme Court concluded that X's privacy rights were not violated in a manner that would have caused personal damage to X in the meaning of Tort Law Act. The dissenting justices concluded that X was entitled to compensation because of an invasion of his privacy. As a sidenote, the Supreme Court's decision implies the difficulties relating to the possibilities of receiving damages based on violation of data protection rights which are heightened by the fact that plaintiff carries both, the burden of proof as well as the risk for legal costs.
Proposal of key words for data base	Respect for private life, protection of personal data, freedom of expression, liability of damages, damages, moral damages (emotional suffering)

Case title	KHO 2008:34
Decision date	13.05.2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	13.05.2008/T:1132 Korkein Hallinto-oikeus [Supreme Administrative Court]

Key facts of the case (max. 500 chars)	A. had requested information from the register of the Supreme Administrative Court about cases which had become pending before the Court between 01–21.11.2007 and which were concerning altogether 83 subject matters specified in the request. In particular, A. requested the names of parties and other information needed to identify the parties. During the period of 01–21.11.2007, 100 cases had become pending pertaining to the 83 subject matters listed by A. The Supreme Administrative Court considered, as far as the 100 cases were concerned, whether the entries marked in the register of the Court and the data needed to identify the party or other person involved in the case were public at the time A.'s request was made or whether such information was to be kept secret on the grounds listed in section 5 of the Act on the publicity of court proceedings in administrative courts (381/2007).
Main reasoning/argumentation (max. 500 chars)	According to section 4(1) of the Act on the publicity of court proceedings in administrative courts, basic information on proceedings in administrative courts, as entered in the court register, is in general public regardless of secrecy provisions. Such public information includes the information needed to identify the party or other person involved in the case as well as information on the authority that has made the decision subject to appeal.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The case concerns balances between publicity of court proceedings and protection of personal information. It also defines the significance of different sources of information in terms of protection of personal data.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The applicant was entitled to receive information on the data needed to indentify the party or other person involved in the case in all but those cases where the secrecy of the data was necessary due to the fact that the data, in combination with the register of the Supreme Administrative Court or a significant information availaible in the decision of the Court would disclose information that ought to be kept secret according to Section 5 of the Act on the publicity of court proceedings.
Proposal of key words for data base	Public documents, trial documents, administrative process, information needed to identify the party, register of an administrative court, document files

Case title	Kuopion hallinto-oikeus 07.06.2007 07/0220/3
Decision date	07.06.2007
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	Kuopion HAO 07.06.2007 07/0220/3 Diaarinumero: 00572/07/1204 Antopäivä: 07.06.2007 Taltio: 07/0220/3 [Kuopio Administrative Court]
Key facts of the case (max. 500 chars)	The case was concerning the question whether the National Board of Patents and Registation of Finland had a duty to erase from the trade register erroneus personal data at the request of the DPO, who, by an earlier decision, had ordered the National Board of Patents and Registration to do so on the basis of sections 29 and 40 of the Personal Data Act (523/1999). The National Board of Patents and Registration requested the administrative court to repeal the decision of the DPO on the grounds that the applicable law in this case was the Trade Register Act (129/1979) and its sections 22 and 23 which provide that erroneus data can be erased from the trade register on the basis of a court decision only. The National Board of Patents and Registration also claimed that the Trade Register Act was *lex specialis* as compared to the Personal Data Act. The administrative court rejected the appeal.
Main reasoning/argumentation (max. 500 chars)	In its decision, the administrative court noted that the Trade Register Act was enacted some 20 years before the Personal Data Act. Since that time the circumstances in which the provisions on the trade register are applied have changed. Because of fundamental rights protection, the Council of Europe conventions on human rights and data protection as well as Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, data protection has become an essential element in the processing of personal data. The administrative court held that, because the basis for the enactment of section 29 of the Personal Data Act is different from the circumstances prevailing during the time sections 22 and 23 of the Trade Register Act were drafted, the National Board of Patents and Registration, as a controller of the trade register, was under an obligation to erase the erroneous personal data from the register on the basis of section 29 of the Personal Data Act, in spite of the fact that the person to whom the personal data pertains could also have made use of the procedure under the Trade Register Act.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Personal Data Act may override more specific conflicting legislation because it is based on constitutionally and internationally guaranteed protection of personal data.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Administrative Court dismissed the application of the National Board of Patents and Registation. In effect the Board was under obligation to erase from the trade register erroneus personal data.
Proposal of key words for data base	Data protection, respect for private life, personal data, fundamental rights, trade register, register entry

Case title	PeVL 29/2008 vp
Decision date	13.11.2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	PeVL 29/2008 vp Perustuslakivaliokunta [Constitutional Law Committee of Parliament]
Key facts of the case (max. 500 chars)	The Government had submitted a Bill proposing the amendment of the Act on the Protection of Privacy in Electronic Communications (516/2004) to the effect that a company or organisation, which subscribes to a communications service and processes users' confidential messages, identification data or location data in its communications network, would under certain circumstances have a right to process identification data in order to investigate unauthorised use of a fee-based information society service or a communications network, the use of a communications service in violation of instructions, and the disclosure of business secrets. In the opinion of the Constitutional Law Committee of Parliament, the Government Bill was in harmony with the Constitution and could

	be passed following the order prescribed for the enactment of ordinary legislation (as compared to enactment of constitutional legislation).
Main reasoning/argumentation (max. 500 chars)	In its statement, the Constitutional Law Committee held that from the point of view of a company, essential business secrets may be of such great economic significance that considerations pertaining to the safeguarding of company assets and the economical prerequisites for business operations constitute acceptable and weighty reasons for limitations on network communications. The Constitutional Law Committee held that the processing of identification data is the ultimate means and is possible only when it is obvious that there are no other means by which the disclosure of business secrets can be investigated. The Committee also emphasised that under section 8(3) of the Act on the Protection of Privacy in Electronic Communications processing is only allowed to the extent necessary for the purpose of such processing and it may not encroach on the confidentiality of messages any more than is necessary. Processing is thus allowed for example only to the extent the company can provide sufficient grounds in order to report an offence or to request for a police investigation. When interpreted and applied in this manner, the provision will not be problematic from a constitutional law perspective, the Committee concluded.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Government Bill is concerning the granting to a private actor — who is often an employer — the right to process, under certain circumstances, identification data associated with electronic communications between another private actor and a third party. The employer is thus not a party to such confidential communications. The Constitutional Law Committee held that under the circumstances as proposed in the Bill, the provision shall not be assessed in the light of the limitations clause in section 10(3) of the Constitution, because this limitation clause in the first place concerns measures by public authorities. In considering the proportionality of the limitations on constitutional rights, the Committee assessed in particular a private actor's need for information in view of the purpose of the provision. Extending the access to necessary and proportional — in that case incomplete — data only is not, in the Committee's view, problematic with regard to the inviolability of confidential communications as prescribed in section 10(2) of the Constitution. Whereas providing a private actor with an even more extensive access to data would have required that the limitations clause in section 10(3) of the Constitution is taken into account.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Constitutional Law Committee of Parliament found the Government Bill to be in harmony with the Constitution. Hence, it could be passed following the order prescribed for the enactment of ordinary legislation (as compared to enactment of constitutional legislation). The case implicates that the constitutional guarantees of personal data enjoy only limited protection in the relations between private persons.

Proposal of key words for data base	Data protection in the work places,

Case title	EOAK 278/2005 Tietovuodot poliisista/Informationsläckar från polisen
Decision date	30.10.2008
Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	EOAK 278/2005 30.10.2008 Eduskunnan oikeusasiamies [Parliamentary Ombudsman]
Key facts of the case (max. 500 chars)	Following findings during the regular supervision of legality, Parliamentary Ombudsman investigated on her own initiative how the police force is trying to prevent the dissemination of secret information and what it intends to do to make investigation of leaks more effective. The police admitted in their reports to the Ombudsman that leaks happen. However, the reports also state that what is often involved is incaution. The police regard actual deliberate leaks to, e.g., news media as rare.
Main reasoning/argumentation (max. 500 chars)	The Ombudsman pointed out that information leaks can cause individuals major and irreversible harm. In addition, they may adversely affect investigation of crimes. That is why there must be a special concentration on investigating leaks, although investigating suspected crimes is challenging in view of such factors as journalists' protection of sources.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Ombudsman stresses that lawful and open dissemination of information by the police in the course of criminal investigations is not a problem. The authorities are required to provide information as openly and actively as possible. The case does not amount to illegal disclosure of confidential information if it may be reasonably argued that the social prominence of some or other person suspected of a crime is a compelling reason to release information concerning that criminal investigation — irrespective of the harm that disclosure of the information may cause the suspect. Instead, what is important is that something that the law requires to be kept secret is not publicly disclosed.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Ombudsman asked the Ministry of the Interior's Police Department to inform her, by 02.02.2009, of how the measures recommended by a working party appointed by the police command echelon to study oversight of the legality of use of register data have been implemented in practice and according to what timetable the intention is to adopt the measures that have not yet been implemented. In addition, the Police Department must report on any measures arising from suspicions expressed by certain provincial command echelons of the police that there are shortcomings relating to cooperation between police and journalists. Ombudsman recommends regulations to clarify procedure for handling personal data.
Proposal of key words for data base	Privacy, secrecy of criminal investigations, openness of government activities, cooperation between police and journalists.

Case title	EOAE 441/2005 Henkilötietojen käsittely kuntien verkkotiedottamisessa/Behandling av personuppgifter i kommunernas nätkommunikation
Decision date	28.03.2007

Reference details (reference number; type and title of court/body; in original language and English [official translation, if available])	EOAE 441/2005 28.03.2007 Eduskunnan oikeusasiamies [Parliamentary Ombudsman]
Key facts of the case (max. 500 chars)	Parliamentary Ombudsman investigated on her own initiative the problems relating to practices of certain municipalities in handling personal data when they are providing information via the Internet. Based on individual e-mail letters to the supervisors of legality, it appeared that there existed clear shortcomings. Details of maternity leave and childcare leave for named officials as well as on individuals' state of health or their being granted disability pensions have been published on municipalities' web sites. Also details of children's applications for school places and school transport as well as of damages claims with individualised supporting reasons have likewise appeared on the Internet. Minutes had remained on web sites for as long as several years.
Main reasoning/argumentation (max. 500 chars)	Personal data may be processed only if doing so is required in the performance of a task or the discharge of an obligation specified in the Personal Data Act. The Court of Justice of the European Communities has found that references to persons on Internet sites or identifying them either by name or otherwise must be regarded as constituting the entirely or partly automated processing of personal data to which the Data Protection Directive refers.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The provisions of the Local Government Act with respect to participation by municipal residents and the provision of information to them require municipalities to observe the principle of publicity in the management of collective affairs. In many cases, however, what is involved in municipal decision making is an application or other matter relating to an interest or right of an individual office-holder or municipal resident or other client of its administration. Then, an assessment must be made in each individual case to determine whether the obligation to provide information as provided for in the Local Government Act is the kind of statutory task or obligation that would justify publishing or dealing with the personal data in question on the municipality's web site. The assessment that must be made in the case is whether posting these personal data on an open information network is necessary from the perspective of the purpose of the municipality's provision of information. In addition, the

	secrecy provisions of the Act on the Openness of Government Activities must be taken into consideration in the assessment.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	In the Ombudsman's view, there might be a need to draft regulations to clarify the procedure to be used when handling personal data in Internet-based communications. Therefore, she proposed that the Ministry of the Interior consider whether there are grounds for ensuring the implementation of data protection by legislative means. The administrative regulations mentioned in the Local Government Act could be required to give explicatory instructions concerning the way personal data are handled in a municipality's provision of information through the Internet, especially from the perspectives of the Personal Data Act and the Act on the Openness of Government Activities.
Proposal of key words for data base	Personal data, local government, minutes of municipalities, Internet