

**OFFICE OF THE DATA PROTECTION OMBUDSMAN**      **March 2009**  
Finland

Data Protection Directive/Article 29 Working Party  
Annual Report 2008

**A. Implementation of Directives 95/46/EC and 2002/58/EC**

The Directive 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 (95/46/EC) was enacted in Finland with the Personal Data Act (523/1999), which entered into force on 1 June 1999. The Act was revised on 1 December 2000, when provisions on the Commission's decision-making, as well as how binding these decisions are in matters concerning the transfer of personal data to countries outside the Union under the Data Protection Directive were incorporated into it.

Protection of privacy has been a basic right in Finland since 1 August 1995. Under the Finnish Constitution, protection of personal data is regulated by a separate act.

The Act on Data Protection in Electronic Communications (516/2004), which entered into force on 1 September 2004, implemented the Directive on Privacy and Electronic Communications (2002/58/EC). The purpose of the law is to ensure confidentiality and protection of privacy in electronic communications and to promote information security in electronic communications and the balanced development of a wide range of electronic communications services.

The responsibility for enforcing the law was divided so that the mandate of the Office of the Data Protection Ombudsman includes: regulations on processing location data, direct marketing regulations, regulations on cataloguing services, and regulations on users' specific right to obtain information.

In this connection, it should be noted that according to the Penal Code, the prosecutor is obliged to consult the Data Protection Ombudsman before pressing charges in a matter concerning a violation of the secrecy of electronic communication.

*Amendments*

During the year under review, there were no actual amendments to the Personal Data Act (523/1999) but provisions pertaining to personal credit data were extracted from it to form an Act in their own right. The transition period of the Credit Data Act ended on 1 November 2008. In part, the Act provides data protection also to legal persons and specifically requires that the data controllers have sufficient data protection competence at their disposal. A new chapter, 5a, was included in the Act on Protection of Privacy in Working Life, which provides detailed provisions on the use of personal credit data in working life.

During the year under review, the amendments required by the directive (2006/24/EC) were entered in the Act on the Protection of Privacy in Electronic Communications (516/2004). The deadline for their implementation will end on 15 March 2009.

In 2006, the Finnish Parliament demanded that the Government begin preparation of legislation on the general protection of personal data in biometric identification. According to the Ministry of Justice, which is responsible for preparing the Act, the general provisions on the processing of biometric identification will be prepared in conjunction with the general review of the Personal Data Act (95/46/EC 8 art 7 paragraph) to be commenced later.

## **B. Major case law**

On 17 July 2008, the European Court of Human Rights gave its ruling in the matter of I vs Finland (no. 20511/03). The matter pertained, among other things, to a person's right to find out on the basis of log data who has had access to her patient records. The Finnish legislation requires taking care of data protection in part to specifically ensure that access to this kind of information can be ensured. However, the data system of the hospital was implemented in such a way that the administration of access rights and the log file could not indicate in detail the persons who had processed data on her. Due to this, and applying the principle of obligatory prosecution, the criminal court could not convict any one person of a crime. In its ruling, the European Court of Human Rights said that a situation has occurred, caused by functional characteristics of a data system that was not controlled as provided in the law, in which the protection of the personal life of the person in question as enacted in the Article 8 of the European Convention on Human Rights has been violated. The decision is particularly significant because the European Court of Human Rights applied the Convention on Human Rights to an electric data system and its deficiencies.

The Court of Justice of the European Communities (the Grand Chamber) gave its ruling on the publication of data on earned income on 16 December 2008. The matter pertained to the scope of application of Directive 95/46/EC, the processing and mobility of personal data on taxation, protection of individuals and freedom of speech. The Court left the definition of the journalistic processing as referred to in Article 9 of Directive 95/46/EC to be done by a national court. On the other hand, according to the ruling, the Data Protection Directive must be applied to the processing of personal data derived from public data sources and the use of previously published lists or services. The matter is still being processed in the Supreme Administrative Court in Finland.

The competent Data Protection Board gave its decision on the matter initiated by the Office of the Data Protection Ombudsman on the authentication of quick loan applicants via mobile phone. In its decision, the Data Protection Board ruled that the practice whereby the creditor identifies the loan applicants solely on the basis of the name, social security number, address and telephone number data provided via a text message that is accepted as a loan application, cannot be considered as a sufficiently reliable practice. Therefore, the Board prohibited the respondent, who followed an authentication process commonly used in the sector, from processing personal data in the aforementioned manner. The respondent complained about the decision of the Data Protection Board to the relevant appeal court. Partly due to this case, a proposal to enact a general law on authentication was put forward in Finland.

## C. Specific issues

### *Attention on special laws*

According to section 10 of the Finnish Constitution, the data protection of personal data must be enacted in law. Due to this provision, there are currently up to 650 special laws legislating on the protection of personal data. With regard to the transfer of data between authorities, the general law to be applied alongside the Data Protection Act is the Act on the Openness of Government Activities. The tragic school shootings in Jokela and Kauhajoki highlighted the issue of the functioning of the whole legislative framework. Particular attention was paid to legislation on student welfare, firearms and health care. It was established that the authorities in various administrative sectors have not paid sufficient attention to the state of legislation. On the other hand, it was easy to observe that personnel who have to apply legislation at the local level have not received sufficient information and steering. Therefore, in problem situations, they were unable to act within even the permitted limits of legislation.

### *Surveys conducted*

During the year under review, the Office of the Data Protection Ombudsman conducted several surveys. The national act on the electronic processing of client data within social welfare and health care entails a specific provision to appoint a person responsible for data protection in each unit. In addition, the act requires that the manager of each unit draws up specific, applicable data protection guidelines. According to our survey, the implementation of the provisions has started off well but the situation could still be improved. At the same time, wide-ranging education for persons responsible for data protection was launched, which at its most comprehensive is university level.

In the so-called web police survey, we analysed the legality of processing personal data in Finnish web-based services. The survey focused, for example, on services providing social networking, services for children and young people and services collecting sensitive personal data. The results of the survey showed that a great deal remains to be done with regard to the fulfilment of the information obligation. Special measures were applied to some of the service providers surveyed.

Our third survey assessed the functioning of the Personal Data Act and partly the criminal sanction system. In our survey, we analysed, among other things, the sentences passed by courts and decisions made by prosecutors. The survey showed that the number of data protection offences continues its slow but steady increase, which is thought to be caused by the improved communication on the rights for and significance of data protection, increasingly secure data systems, and the improved professional competence of the police and prosecutors. On the other hand, there was some discussion on whether the sanction system is strict enough.

### *Scientific research*

Scientific research often deals with sensitive personal data. For research purposes, data is often needed from a variety of sources. In our experience, researchers are often very insufficiently informed on the requirements set by data protection on scientific research. For this reason, we implemented an extensive and comprehensive web-based guidelines project in cooperation with various authorities. The aim of the project was to improve the level of data protection in scientific research, to make researchers' work easier and to improve the practices of authorities functioning as sources of information. The project output includes virtual guidelines together with their requisite quality assurance systems and several manuals determining best practices.