

REVIEW 2003

Contrary to popular belief, the mandate of the **Data Protection Ombudsman** does not include the power to permit or prohibit data processing. It is the Data Protection Board that has such authority. Two cases concerning prohibition were presented to the Data Protection Board in the 16th year of operation of the Office. The first case concerned the new travel card system used in the Helsinki area, and the second concerned a printed catalogue containing the taxation details of over one million people.

The Data Protection Ombudsman learned that the Helsinki Metropolitan Area Council YTV – whose statutory duty it is to organise public transport within the Helsinki metropolitan area – had designed a data system which recorded individual journeys first in the system's remote readers, and then in its central system, with the help of an identification chip in the travel card. The system also recorded personal data, including each card holder's social security number (unless they opted for an anonymous card, which is more expensive). In the opinion of the Data Protection Board, the information generated for YTV from the system was subject to error, and hence YTV must revise the system.

When the matter was processed in the Data Protection Board, YTV announced that it would modify the system so that journeys made by private individuals will no longer be stored in the system, and the relevant matter was dropped. With regard to collecting social security numbers – which YTV had initially justified by saying that it needed the data to collect inspection fees – the Board came to the conclusion that YTV has the right to use social security numbers, since it needs them to verify card holders' domiciles because different municipalities in the YTV region participate in the maintenance of public transport in different ways. The Data Protection Ombudsman did not appeal this decision. During the processing of the matter, YTV acknowledged that it needed to improve the standard of the information it discloses.

In January 2004, the Board gave its statement that the catalogue containing tax information was not in breach of the Data Protection Act. This decision was later appealed in the Administrative Court, and the matter is still pending. The appeal included a request that a competent administrative court would request a preliminary ruling from the Court of Justice of the European Communities.

The year of viruses

2003 was the worst computer virus year ever. Viruses and other malicious programs spread faster and wider than ever before. In fact, they posed a threat to the very infrastructure of Finnish society: a bank had to close temporarily, and the e-mail traffic of a Finnish telecommunications operator was completely jammed.

Fortunately, lessons were also learned. Although these problems undoubtedly raised the awareness of data protection issues among the public, confidence in the security of data networks also suffered. Then again, Finnish society responded swiftly. On the 4th of September, the Government issued a decision-in-principle on the National Information Security Strategy. This strategy is based on the strategy proposal made by the Information Security Advisory Board, which was active between 2001 and 2003. One starting point for the strategy is the protection of citizens' fundamental rights, including the protection of personal data files. The prestigious International RSA Information Security Conference granted an award to the Ministry of Transport and Communications for the best principles in the National Information Security Strategy in the European policy series. The year 2003 was a busy one for the Steering Committee for Data Security in State Administration (VAHTI) operating under the Ministry of Finance. It co-ordinated the drafting and publishing of several guidelines which proved extremely popular among the public. Besides the Data Protection Ombudsman, several experts from the Office of the Data Protection Ombudsman also participated in this work.

The Data Protection Ombudsman was appointed a member of a special advisory group which was established to steer the implementation of the National Information Security Strategy.

Besides viruses, a constant flow of junk e-mail continued to infest mobile phones and e-mail accounts. The majority of this unsolicited mail originates outside Finland, mainly from the U.S. The Market Court issued a

decision in which it specified the concept of "spam". According to the court decision, asking for prior consent required by the law for solicitation via e-mail can be defined as marketing.

In the year under review, a government proposal for the Act on Data Protection in Electronic Communications (HE 125/2003) prepared by the Ministry of Transportation and Communications was submitted to Parliament. The proposal aimed at combating malicious programs and spam. The proposal will transpose Directive 2002/58/EC on Privacy and Electronic Communications of the European Parliament and of the Council, adopted in 2002, in national legislation.

Information society programme – a change of paradigm

In 2003, the number of those who failed to understand the importance of data protection continued to decrease. When the State Audit Office published its performance audit report on the Office of the Data Protection Ombudsman in 1998 (VTV/Tarkastuskertomus 8/98) it titled the 7th section, dealing with data protection and co-operation among different authorities: "Data protection and the development of data processing – does the protection of privacy restrain the utilisation of IT resources by public authorities?"

The State Audit Office answered its question in a way still true today: "The benefits brought by automatic data processing cannot be utilised to the maximum of what legislation in force would allow. One of the central reasons for this is deficiencies in internal special legislation in different administrative branches."

The change in paradigm is well-illustrated by a concept taken from the Information Society Strategy, then incorporated into the government's programme: "Citizen and enterprise trust in the information society should be enhanced by improving data protection and the protection of privacy." The Data Protection Ombudsman was appointed a permanent expert in the Council for the Promotion of the Information Society Through Education, Research and Culture.

2003 marked the transition from the Fifth to the Sixth Framework Programmes in the European Union. In its assessment, the Commission draws a number of conclusions, such as the following:

- privacy will be increasingly emphasised;
- public awareness is at an insufficient level;
- legislation needs to be amended, and
- new online data protection models should be developed and business models should be revised with the help of data protection.

Assessment concerning the technical requirements of the Commission lists the following issues:

- more education is needed and public awareness should be raised;
- management measures are needed to translate data protection into an active part of system planning;
- the basics of data protection should be made a basic part of business processes;
- IT infrastructure to support data protection should be developed;
- user-friendliness is a requirement for all technology supporting data protection (PET technologies); and
- technology must benefit users and prevent breaches of data protection.

These estimates of the Commission can be crystallised in the idea to integrate the prerequisites of personal data legislation more closely into basic data file processing.

However, this integration will fail unless controllers, organisation management, experts, and other people processing personal data have sufficient skills and competence and are also able to understand the activities in other sectors, and have a good technological knowledge. The Data Protection Ombudsman aims to meet this challenge better than ever before. Office operations were revised with regard to the maintenance of personnel skills: separate internal meetings on legislation and theme meetings are now arranged every month. Obligatory training, that is, the compulsory attendance of personnel at training to enhance their

professional skills, continued. The themes of training provided for the entire personnel included interaction and communications skills, and data protection.

Perspective of the data subjects

The Office of the Ombudsman for Aliens carried out an open public questionnaire in connection with the 'Registers open' event. There were 117 respondents. The preliminary results indicated that:

- 58% of the respondents had not been informed by organisations who had gathered their personal data,
- 78% thought that income/tax information were private issues,
- 63% thought that electronic transactions were unsafe,
- 63% accepted the GPRS location of minors under 15 years of age,
- 55% were in favour of drug screening in schools,
- 61% thought that mobile phones with cameras pose a threat to their privacy,
- 48% would agree to have their fingerprints taken for access control at work,
- 81% opposed the reading of their e-mail by someone else at work, and
- 52% opposed the establishment of a national gene bank.

The questions were deliberately drawn up in yes/no format. More often the issue is how something is done, rather than is it done at all.

The year saw several court cases on data protection which undoubtedly affected public opinion. Data protection and data protection violations in the telecommunications sector and the dispute between the EU and the U.S. over the transfer of data by airlines to the U.S. administration are examples of such cases. In autumn, Finnair Oyj began to disclose PNR (Passenger Name Records) to the United States, but informed the passengers of this in advance, and asked their consent for the transfer. The U.S. has threatened to impose sanctions, or even refuse landing permission in its territory in case of failure to disclose information to an official request. Investigation into the case of suspected violation of telephone privacy of employees revealed that there were telecommunications operators who had not protected telecommunications information, even with a log system. The Finnish Communications Regulatory Authority (FICORA) whose tasks include monitoring telecommunications service providers and communications privacy in particular, soon required clarification on the matter.

Although issues and occurrences related to data protection continued to be reviewed extensively in the media, the level of citizens' awareness of their rights in data protection lagged behind. This is naturally a great challenge for our office communications. For this reasons, the office began to revise its web site and to implement a communications plan, in compliance with the Act on the Openness of Government Activities, and adopted by the Data Protection Ombudsman in June.

The Data Protection Ombudsman submitted a total of 21 statements to prosecutors and courts of law (in 2002, there were 14 requests for statements from legal bodies). Despite the increasing number of requests, application of the law continues to be inconsistent among prosecutors and courts of law. This issue must be addressed in the future. The fact that only 90 cases concerning right of access and erroneous information were brought before the Office by data subjects (in 2002, 124 cases) can, however, be described as a positive development. The Data Protection Ombudsman gives a decision in these matters and they can be further appealed in administrative courts and the Supreme Administrative Court. The average time for processing requests for the right of access and rectifying erroneous information at the office was six months (in 2002, also six months). The Office had a total of 1,794 matters pending (in 2002, 2,017), and 682 issues were transferred for handling in 2004 (in 2002, 998 issues). The year under review was the first in the entire history of the office when the number of matters decreased compared with the previous year.

Increasing internationalisation

The Office of the Data Protection Ombudsman spends 10% of working hours dealing with international affairs. Thus, this is an upward trend.

The aim of the Personal Data Act and the underlying Data Protection Directive is to secure legal data transfers within the EU and EEC territories and, secondly, to oversee that personal data is transferred outside these areas only if an adequate level of data protection can be guaranteed.

Both Finnish enterprises and foreign enterprises established in Finland increasingly outsourced their operations outside the Member States. To facilitate such development, the Commission of the European Union adopted two model contract clauses which enable the enterprises to guarantee an adequate level of data protection. From the viewpoint of national legislation, it also seems that enterprises have flexible mechanisms for data transfer which ensure the protection of data subject's rights quite well. It should be noted, however, that the business concepts of those in charge of transfers or involved in them – with their outsourcing and subcontracting arrangements – are often so complicated that model clauses can be rarely used as such. The fact that enterprises have to comply with national legislation in all transfers adds an extra dimension to the writing of contract clauses. Thus, the issues concerning data transfer to third countries are often judicially challenging and, in practice, time-consuming.

The meeting of the Nordic Offices of Data Protection Ombudsmen was held in Helsinki in August. Despite more extensive international co-operation and new forms of it (such as the utilisation of an intranet), the meeting decided it was appropriate to continue, and even enhance, Nordic co-operation in this form. The meeting agreed on the start of Nordic auditing and a working group, led by Sweden (who made the proposal), was established to develop it. Later on, the Nordic Data Protection Ombudsmen agreed on the theme of inspection which was the processing of personal data in employee recruitment. The actual auditing and related reporting will take place in 2004.

Preliminary rulings on the cases presented by the Göta Court of Appeal, Sweden (C101/01) and the Austria case (C 165/01) by the Court of Justice of the European Communities shaped the interpretation of data protection legislation, and were thus part of international activities.

On social impact

The statutory duties of the Data Protection Ombudsman in Finland include supervision of the processing of personal data in our country, the resolution of cases related to the right of access and rectification of personal data, data protection inspections, guidance and advice for private individuals and controllers, and international affairs. Moreover, the authorities are obliged to consult the Data Protection Ombudsman in law-drafting and administrative reforms. Our office also participates in the work of various committees and working groups.

The Data Protection Ombudsman conducts performance negotiations with the Ministry of Justice annually, which has an effect on the budget. We have mainly used two indicators in the negotiations to measure the results of our work. Indicators are the number of cases solved and the length of time it takes to process a case, in months.

Initially, we wanted to learn how well we had managed to meet the challenges of our extensive mandate, and how firmly our office had established itself in Finnish society. We first specified the chosen viewpoint by creating indicators which would help to show the development of trends in our activities, and which would serve as indicators, helping us to react to future changes.

We upgraded our values, visions, and strategies. Using these as a starting point, we determined the prerequisites for successful operations, and designated each operational section with three key performance objectives. We then created indicators for each key performance objective and determined the goals for them in the near future. Finally, two internal working groups were established to reform our own working routines.