COMMISSIONER
FOR PERSONAL DATA PROTECTION
(CYPRUS)

Year Review
2008

1. Introduction

This is the 6th annual report issued by the Commissioner for Personal Data Protection. It refers to the main activities of my Office during 2008.

These relate to standard activities, e.g. review of the notifications for establishing and operating filing systems submitted to my Office, issue of licenses for combination of filing systems and transfer of personal data to third countries, inspections/ audits carried out and complaints investigated.

At the same time, my office staff has been doing presentations and seminars at the Academy of Public Administration, the Police Academy and other professional organizations and Public Service Departments, upon request or by our own initiative.

Considering the importance given to public awareness about the law and the citizens' rights, but also taking into account the risks that the use of new technologies may involve, particularly in relation to children, we have distributed in secondary schools, colleges and universities a 6-page brochure on the use of Internet and mobile phones.

Regarding the inspections, which aim to identify weaknesses or omissions in the application of the Data Protection Law, audits were conducted in two public hospitals and in addition to that we followed the adoption of our recommendations on the protection of personal data in the New General Hospital.

With the same goal and in response to citizens' telephone calls and complaints, I decided to conduct an investigation involving the bank sector. The audit consisted of a questionnaire sent to all banks operating in Cyprus, which in addition were asked to submit to us all the application forms used by their customers and employees. Their responses will be evaluated and recommendations will be submitted if their policies and practices are found not to be in accordance with the law.
The results of the audit will be published in the 2009 Report.

Goulla Frangou
Commissioner
for Personal Data Protection

2. Statistics

2.1. Notifications

In 2008, the Office of the Commissioner has received 194 notifications about the establishment and operation of a filing system or the commencement of processing of personal data, bringing up the total number of notifications kept in the Commissioner's register to 2132:

Sector	Notifications submitted in 2008	Total number of notifications
Public sector	110	489
Legal entities/ organizations	19	792
Private sector	65	851

2.2. Licenses

Combination of filing systems

"Combination" means a form of processing which involves the possibility of connection of the data of one filing system with the data of a filing system or systems kept by another controller or other controllers or kept by the same controller for another purpose.

According to section 8 of the law, every combination shall be notified to the Commissioner by a statement submitted jointly by the controllers who will combine two or more filing systems which are established for different purposes.

If at least one of the filing systems, which are to be combined, contains sensitive data or if for the combination to be carried out a single code number is to be used, the combination is permitted only with the prior license of the Commissioner.

After hearing the views of controllers the Commissioner has granted 9 licenses in 2008 as follows:

	Controller 1	Controller 2
1	Population and Immigration Registry department	Military Services
2	Inland Revenue department	Social security services
3	Police (firearms filing system)	Military Services
4	Cyprus Security and Exchange Commission	Cyprus Stock Exchange
5	Police	Customs Department
6	Income revenue department	Department of Lands and Surveys

7	Turkish-Cypriot Property Department	Population and Immigration Registry department
8	Labor Office	Social security services
9	Social security services	Social Welfare services

Transmission of data to third countries

According to the provisions of the Data Protection Law, transmission of data which have undergone processing or are intended for processing after their transmission to any country which is not a member of the European Union shall be permitted after a license of the Commissioner.

The Commissioner issues the license only if he considers that the said country ensures an adequate level of protection. For this purpose, he shall take into consideration the nature of the data, the purposes and duration of the processing, the relevant general and special rules of law, the codes of conduct and the security measures for the protection of data, as well as the level of protection in the countries of origin, transmission and final destination of the data.

In 2008 the Commissioner has issued 24 licenses for transfer of data to counties such as the United States of America, Canada, Russia, Switzerland, Lebanon, Australia etc.

2.3. Complaints

The number of complaints submitted in 2008 was 264. The main categories of complaints submitted are as per the table below:

Category/ subject of complaint	Number of complaints	Percentage
Consent/ Right to be informed	**2**	**1%**
CCTV systems/ voice recording	**15**	**5,5%**
Disclosure	**16**	**6%**
Publication/ Media	**3**	**1,5%**
Confidentiality/ Security measures	**6**	**2%**
Right of access/ right to object	**9**	**3,5%**
Spam (e-mail, sms, fax)	**175**	**65,5%**
Direct marketing	**8**	**3%**
Purpose of processing	**7**	**2,5%**
Unauthorized collection (source of data)	**2**	**1%**

Excessive data (principle of proportionality)	**11**	**4,5%**
Biometric data	**1**	**0,5%**
Loss/ destruction of data	**1**	**0,5%**
Unfounded (out of the scope of the law)	**8**	**3%**
TOTAL	**264**	

Most of the complaints submitted concerned unsolicited communications, mainly to mobile phones. Then follows the complaints about disclosure of personal data to third parties and complaints about the installation and operation of closed circuit video surveillance.

3. Major cases

3.1. Spam

In 2008 although the number of complaints for unsolicited communications (spam or junk mail) is still fairly high, many senders have already complied with the law. The major spam cases that the Commissioner's office dealt with was sms advertising premium rate numbers (starting from 900) offering dating and astrological predictions.

Intermediary companies providing mass-messaging services sent these messages or enabled their customers to send messages via the Internet.
We contacted several of these companies and informed them about the legislation provisions and we have furthermore visited their offices in order to find solutions for the problems arising from unsolicited communications.

Our intention is to continue this cooperation in order to arrive at an appropriate framework for providing these services.

We have also requested the companies sending bulk sms to give the recipients an opt-out option, by providing a free phone number for this purpose.

3.2. Close circuit television (CCTV) and monitoring

During last year we received several complaints about the operation of CCTV in offices, shops etc, but also for CCTV installation in private homes or entrances to private buildings and corridors thereof.

Regarding the CCTV installation in houses and building blocks, in most of the cases we were not able to proceed with an investigation for the reason that the Data Protection law does not apply if the processing of personal data is performed by a natural person in the course of a purely personal or household activity.

On the other hand, we have investigated complaints for the establishment and operation CCTV in shops and offices and other workplaces.

According to the guidance issued by the Commissioner in 2005 for the Employment Sector, the employees' monitoring is permitted under the Act only if the employer is able to justify the legitimacy and necessity of monitoring, when no other less intrusive means are available to attain the objectives pursued. Moreover, only exceptional circumstances can justify the permanent surveillance of employees and usually these cases are limited to places where high security measures must be taken or in areas where public health and safety can be endangered (e.g. airports, military infrastructures).

There are five conditions in Data Protection Act for the lawfulness of the processing and as far as monitoring is concerned, the principle of proportionality, which provides that the personal data should be relevant, appropriate and not excessive in relation to the purposes of processing, should apply. The cameras should be placed in such a way to collect only the relevant data, which relates to the purpose of the processing.

A complaint against a car concessionaire company who had installed a CCTV system in the offices, the lobby and the garage, for security reasons, which was submitted by the employees' trade union, was examined.

We found that the cameras were installed in specific areas, mostly in corridors, the warehouse, near the cashiers and outside the premises. In the garage the camera enabled the customers sitting in the lobby to have a direct view of their car while it was being repaired (according to international standards of the Company).
The employer alleged that the CCTV was set up only for security reasons and to protect the company's property from damages and burglary.

The Commissioner considered that a permanent surveillance of staff was not acceptable in this particular case. Even in the garage, the permanent monitoring of employees was not allowed, as the legitimate interests pursued by the controller did not override the rights, interests and fundamental freedoms of the employees. There was furthermore a contravention of the principle of proportionality because the data collected in the lobby and the garage were excessive having in mind the purpose pursued (e.g. to prevent damages and robbery).

A sanction was imposed obliging the employer to remove the cameras from the garage. The Commissioner required that the other cameras should be placed in such a way that no excessive personal data of employees should be processed.

3.3. Complaints and inspections in public hospitals

Following some newspaper articles and complaints in relation to management of patients' files in public hospitals, it was decided to inspect four of them in order to identify any weaknesses in the security measures and then prepare guidelines to be implemented by all medical centers.

Our intention is to carry out similar inspections on private hospitals and clinics in 2009.

Case 1: Loss of a patient's medical file

Following the relocation of the Nicosia General Hospital, thousands of medical files needed to be removed and reorganized. A patient exercised the right of access to his medical data in November 2006. For 6 months his medical file could not be located and the patient submitted a complaint to the Ombudsman who forwarded it to the Data Protection Commissioner for competency reasons.
Until June 2008 the patient's file was not found and the manager of the hospital could not provide any appropriate justification.
In July 2008 the Commissioner imposed to the data controller a fine of €2000 for not satisfying the data subject's right of access.

Case 2: Insufficient security measures at Limassol hospital

A complaint was submitted in 2008 alleging that a patient or a visitor could easily have access to the laboratory results in Limassol hospital. We proceeded to an on spot investigation and we found out that there were insufficient security measures in the laboratory, but also in other premises of the hospital where records were kept (e.g the X-ray laboratory). Moreover, we observed that the hospital did not provide the staff with any privacy policy and the staff (mainly secretaries and nurses) was completely ignorant about the data protection law and their obligations.
A seminar was then organized in Limassol hospital in order to inform the staff about the legislation and their obligations.

Inspections

Our office decided to inspect at least two hospitals for the purpose of ascertaining the progress made on applying the New Electronic Health File System and the security measures.

During the inspection in the Nicosia General Hospital we were informed about the progress in the establishment of the Comprehensive Health Information System (CHIS). After its completion this system will allow an interconnection between all hospitals and medical centers via an electronic communication network (WAN). It provides 2 access levels to the system; depending on the user's functions and duties e.g. the administration desk officer has access only to demographic data. Each user will have a username and a primary key and all information entered into the system will be tracked for security reasons.
The implementation of the CHIS started in January 2007 and will be completed in 2009 in two hospitals.

After conducting the inspections we sent a letter to the Ministry of Health regarding various issues found during the inspections in order to establish a uniform policy to deal with them. These issues concerned primarily the establishment of a common procedure for the security measures to be taken, the classification of the documents entered in the

patients' files and the issuance of common forms (e.g. application forms for exercising the right of access).

All the pending issues will be followed until we obtain satisfactory results.

4. International

The Article 29 Working Party* has decided to carry out the second coordinated enforcement action in all Member States, regarding the implementation of Directive 2006/24/EC of the European Parliament for the retention of data generated or processed in connection with the provision of publicly available electronic communications services or public communications networks and also for amending Directive 2002/58/EC, whose provisions have been transferred in the Retention of Telecommunications Data for the purpose of Investigating Serious Criminal Offences Law of 2007.

The Working Party is also paying particular attention to children's data protection, and will prepare for this purpose an opinion, which it is aimed particularly at those who handle children's personal data such as teachers and school authorities. It is also aimed at national data protection supervisory authorities, who are responsible of monitoring the processing of such data.

As far as justice and security is concerned, we have been following the developments regarding the adoption of the following Decisions that will have to be transposed in the national law before end 2010.

- The Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal affairs, and

- The implementation of decision 2008/615/JHA on the stepping-up of cross-border cooperation, particularly in combating terrorism and cross-border crime

Along with our supervisory activities, we also follow and participate to the works of European Union and Council of Europe committees and bodies. This way we acquire experiences, we learn about the best practices applied and we get information and assistance, for the better implementation of the data protection legislation, in accordance with the Directives and other instruments of the European Union.

* This working party has been established by article 29 of Directive 95/46/EC referring to the protection of personal data. It is independent EU Advisory Body on Data Protection and Privacy.