COMMISSIONER
FOR PERSONAL DATA PROTECTION
(CYPRUS)

Year Review
2007

1. Statistics

1.1. Notifications

In 2007, the Office of the Commissioner has received 90 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 to 1938:

Sector	Notifications submitted in 2007	Total number of notifications since 2002
Public sector	36	379
Legal entities/ organizations	2	773
Private sector	52	786
TOTAL	**90**	**1938**

During the last few years, the number of CCTV (close circuit televisions) systems established and operating in Cyprus significantly increased. Although 52 notifications have been submitted at the Commissioner's Office, we believe that there are still many CCTV systems, for the operation of which no notification has been submitted.

Sector	Notifications for CCTV until 2007
Public sector	14
Legal entities/ organizations	5
Private sector	33
TOTAL	**52**

2.2. Complaints

The number of complaints submitted in 2007 increased to 220:

Category/ subject of complaint	Number of complaint	Percentage
Consent/ Right to be informed	**6**	**3%**
CCTV systems	**21**	**9,5%**
Disclosure	**27**	**12%**
Confidentiality/ Security measures	**2**	**1%**
Right of access/ right to object	**8**	**4%**
Spam (e-mail, sms, fax)	**110**	**50%**
Direct marketing	**2**	**1%**
Purpose of processing	**5**	**2%**
Source of data	**5**	**2%**
Excessive data (principle of proportionality)	**16**	**7%**
Period of retention/ deletion of data	**2**	**1%**
Application of the law	**5**	**2%**
Biometric data	**1**	**0,5%**
Unauthorized access	**2**	**1%**
Complaints out of the scope of the law	**8**	**4%**
TOTAL	**220**	

2. Major cases

2.1. Spam

Most of the complaints submitted involved spam messages where the sender's contact details were not available. These messages asked people to call or send a message to a premium rate number.

In order to locate the sender of the message we ask the telecommunication service providers for the contact details of the owners of these numbers. Delays often occurred while waiting for the service provider's reply, and this negatively affected the prompt investigation of the complaints.
The service providers have been requested to appoint a contact person to speed up this process.

In many cases, an additional step was required for their investigation, where the service provider (which in most of the cases is the Cyprus Telecommunications Authority) has leased the numbers to another company, which in turn has sub-leased the numbers to its customers. This introduced further delays until we contacted the last company to receive the details of its customer.

Many spam cases have been investigated where the senders allege that they have obtained the recipient's consent via a website where the recipient had registered and the terms and conditions of that website state that the persons who register agree to receive advertising messages. This practice is not lawful as the consent should be explicitly given (it could not be implied) and also freely given (it could not be part of the terms and conditions of a service or a contest).

A spam case involving the sending of unsolicited communications to mobile phones relating to horse racing results was investigated after a number of complaints submitted to the Commissioner. The messages were sent (by several numbers) using prepaid telephone cards.
The sender of these messages never responded to our letters or answered our questions and after following the prescribed procedure, the Commissioner proceeded to issue a Decision imposing on him a fine of C£2000.

2.2. Biometric data

The use of biometric data has been the subject of various international and European bodies and it is also regulated by a document adopted by the Article 29 Working Party[1] of 2003.

[1] 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.

Biometric data are the physical and physiological characteristics of a person and include: fingerprints, finger image, face recognition (photo), iris recognition, retina analysis, outline of hand patterns, body odour, voice, DNA pattern analysis etc.

It is often used in automated authentication and identification procedures, in particular for control of entry to both physical and virtual areas (to particular electronic systems or services).

The provisions of Data Protection Law apply to the collection of biometric data and therefore the processing of these data is lawful only if it is carried out according to the provisions of Data Protection Law.

The collection of biometrics, and especially the fingerprints, is mainly used for law enforcement purposes (e.g. criminal investigation). According to the Data Protection Law personal data must be **collected for specified, explicit and legitimate purposes and should not further processed in a way incompatible with those purposes.** Also, according to the principle of proportionality personal data must be **relevant, appropriate and not excessive in relation to the purposes of processing.**

In 2007 a case was investigated regarding the introduction of a biometric system by a data controller who was using the employees' fingerprints for time registration purposes. The employer had used other systems before but found them to be open to fraud and misuse.

It was decided by the Commissioner that the collection and use of fingerprints for this purpose was not in accordance with the Law as this method should only be used in exceptional circumstances, e.g. where additional security measures to control access to the premises are deemed necessary.
The controller was asked to discontinue this kind of processing and destroy the fingerprints already collected.

2.3. Collection of medical data by Insurance Companies

A lot of complaints were received for the last 2 years against Insurance Companies that offered health insurance contracts, which requested the medical and lab results of their clients in order to satisfy their claims.

The Insurance Companies alleged that this practice proved to be necessary in order to avoid fraudulent and/or non-existent claims by the insured.

The Commissioner had several meetings with the Insurance Companies involved and submitted the following suggestions:

- The standard practice of the Insurance Companies should not be to ask for the submission of the medical results of the insured in all cases.

- The Insurance Companies are not authorized to request the medical results of routine checks of their clients.
- For any other claims, the Insurance Companies may request medical results solely when it is absolutely necessary in order to decide if the compensation falls under the terms of the contract or in order to evaluate the amount of the compensation.

2.4. Security measures for health records at the old Nicosia Hospital

After a publication in a daily newspaper in March 2007, which referred to the situation prevailing at the old Nicosia General Hospital (after its relocation to a new building), the Commissioner decided to carry out an investigation.

The investigation revealed that documents containing personal data of patients were left in certain parts of the old Hospital and no access control existed despite the presence of guards at the entrance to the Hospital. Consequently any person, including those who were carrying out repairs, could enter the building and have access to these documents.

Explanations were given by representatives of the Ministry of Health, which was responsible for the relocation of the Hospital, regarding the security measures and the data left at the old premises.

Thereafter measures were taken to prevent unauthorized entrance to the premises and the documents found therein were taken to a safe place and/or destroyed.
Taking into account the fact that there was compliance with the directions of the Commissioner, a fine of C£1500 was imposed on the Director-General of the Ministry.

3. Important events

3.1. Spring Conference of the European Data Protection Authorities

In May 2007 the Commissioner's Office organized the annual Spring Conference of the European Data Protection Authorities in Larnaka, Cyprus. 109 representatives from 47 accredited European National and Sub-National Data Protection Authorities and Authorities within an International or Supranational Body, non-accredited Authorities with the status of an observer and Authorities invited by the Organizing Authority attended the Conference.

The Conference's agenda included topics on electronic health records, the future of data protection and the Police Working Party, current developments about data protection in

the third pillar and in EU Institutions, media and other issues regarding children and personal data, trans-border data flows and the fight against terrorism.

The works of the Conference were concluded with the adoption of a Declaration on the Common position of the European Data Protection Authorities on the use of the concept of availability in law enforcement, a Declaration regarding the Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation and a Decision on the future of the Police Working Party.

The above Declarations were sent to the German Ministers of Justice and Home Affairs, the Director General and the Vice President for Freedom, Security and Justice at the European Commission, the Chairman of the LIBE Committee, the President of the European Parliament and the Chairman of Article 36 Committee. Additionally the Data Protection Authorities were asked to send these two documents to their relevant national authorities in order to raise awareness on the Conference's conclusions on the above subjects.

3.2. European Data Protection Day

In October 2006 the Council of Europe decided to establish the 28th of January as European Data Protection Day in order to raise awareness for citizens' rights in this area and to commemorate the opening day for signing Convention 108, the first European data protection legal instrument.

On the first European Data Protection Day in January 2007 the Commissioner's Office organized a number of events, which included a press conference, a television broadcasted message and the distribution of relevant flyers in a Nicosia central avenue. The distributed posters and flyers had the message *"Personal data protection. It concerns us all*".