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

## Cyprus Report

By Corina Demetriou & Nicos Trimikliniotis

Deadline: 2 February 2009

# Contents Structure

# Executive Summary

[1]. The Cypriot Data Protection Authority, named by the relevant law as the Commissioner for the Protection of Personal Data, was set up in 2002 by the Processing of Personal Data (Protection of the Individual) Law of 2001 and amended in 2004 and has operated since May 2002. The role of the Commissioner is to safeguard personal data by protecting personal information relating to an individual against its unauthorised and illegal collection, recording and further use and it also grants the individual certain rights, such as the right of information, the right of access and the right of objection and provides for the procedure of submitting complaints to the Commissioner for violations of the law. The Commissioner may impose on the controllers or their representatives a number of administrative sanctions and has on a number of occasions made use of this right. Since its inception, the office of the Commissioner for Personal Data Protection publishes annually a report setting out its activities; the latest published annual report concerns the year 2007.

[1]. The Processing of Personal Data (Protection of the Individual) Law of 2001 vests the Commissioner with fewer powers than required by Article 28 of Directive 95/46/EC. The powers granted to the Commissioner include the right to be consulted in the preparation of regulation or the adoption of measures, if requested, investigative powers and powers of intervention. However, the Commissioner does not have the power to engage in legal proceedings or to bring violations to the attention of judicial authorities. The European Commission has notified that there are sections of the Processing of Personal Data Law of 2001 that do not comply with the European Data Protection Directive including the provisions on the right of information, transfer of data to third countries and other procedural mechanisms. The Data Protection Authority has drafted amending legislation which purports to bring the law in line with the Directive but it is yet to be tabled in Parliament.

[2]. A problematic area in the institutional framework of the data protection authority is the fact that the staff consists of public servants falling under the administration of the Public Service and the Statistical Service, whilst the Data Protection Commissioner is not involved in their selection or in the determination of their required qualifications. The Commissioner is of the opinion that the current procedure, which leaves her with no opportunity to select the most suitable staff, is compromising the independence of the institution and its effective functioning. An additional limitation of the data protection authority is the fact that it is underfunded and understaffed.

[3]. In addition to the limitations indicated above, one of the main obstacles facing the data protection authority is the lack of mechanism to address the problem of non-cooperation by controllers of personal data or by third parties during investigation of complaints or during self-initiated investigations conducted by the Commissioner. The data protection authority has proposed amendments to the law to address this procedural weakness.

[4]. In general there is a good record of compliance with the recommendations of the authority. However, the authority cannot monitor compliance in every case it handles.

[5]. Since 2002, the data protection authority has been involved in various awareness raising activities such as number of press conferences, open seminars to the public, as well as lectures by officers of the authority to organisations in the private and in the public sector. Also, there are various websites offering information regarding data protection, including the website of the Cypriot data protection authority. However, there are no studies and/or surveys on the level of awareness regarding data protection law and rights in Cyprus.

# 1. Overview

[6]. The Cypriot Data Protection Authority was established in 2002 on the basis of the Processing of Personal Data (Protection of the Individual) Law of 2001 as amended in 2004. The office of the Commissioner for the Protection of Personal Data is named as the institution empowered and obliged by law to fulfil the task of safeguarding personal data by protecting personal information relating to an individual against its unauthorised and illegal collecting, processing and maintaining such data. Moreover, the above mentioned law grants individual rights, such as the right of information, the right of access and the right of objection and provides for the procedure of submitting complaints to the Commissioner for violations of the law. The Commissioner is responsible for monitoring and safeguarding such rights and may impose on the controllers or their representatives a number of administrative sanctions and has on a number of occasions made use of this right. The main impetus for the establishment of the Data Protection Authority was the harmonisation process in the light of accession to the EU and compliance with the EU acquis under Directive 95/46/EC of 24 October 1995 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data as well as other provisions that are part of

the EU acquis.[1] However the Cypriot law does not fully comply with the EU acquis; there is currently a draft legislation to amend the original law.

[7]. Constitutionally the functions of the Data Protection Authority fall within the wider remit of human rights protection and in particular the right to privacy and private life based on constitutional and international standards relevant for data protection in Cyprus. The right to private and family life is safeguarded by article 15 of the Cypriot Constitution and article 8 of the ECHR to the extent that the processing of personal data adversely affects the private and family life. Moreover, article 17 of the Cypriot Constitution provides that every person has the right to respect for, and to the secrecy of, his correspondence and other communication, if such other communication is made through means not prohibited by law. Also a number of international instruments provide the standards for these rights such Council of Europe instruments [2] and other UN instruments.[3]

[8]. The Commissioner for the Protection of Personal Data is the only body which specialises on the subject and has powers and personnel to monitor the collection and processing of personal data. Prior to the establishment of this institution there was no other body responsible, except for the general Courts who have jurisdiction to enforce the law and safeguard human rights and, to some extent, the Commissioner for Administration (ombudsman) to the extent that this institution is granted powers for safeguarding private life from abuse and maladministration by public authorities.

[9]. The powers granted to the data protection Commissioner include the right to be consulted in the preparation of regulation or the adoption of measures, if requested, investigative powers and powers of intervention. The office of the data protection Commissioner publishes annually a report setting out its activities. However, the Commissioner does not have the power to engage in legal proceedings or to bring violations to the attention of judicial authorities.

[1] Such as Regulation 45/2001/EC and Directive 2006/24/EC.

[2] Recommendation Rec(87)15 addressed by the Committee of Ministers to the Member States of the Council of Europe, regulating the use of personal data in the police sector, adopted by the Committee of Ministers on 17 September 1987, at 401st meeting of the Ministers' DeputiesThe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981). 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).The Convention on Human Rights and Biomedicine (1997), especially its Article 10 on 'Private life and right to information'.

[3] such as Article 17 of the International Covenant on Civil and Political Rights (ICCPR, 1966) and the General Comment No. 16 on Article 17 ICCPR (especially its paragraph 10 on personal data).The Guidelines for the Regulation of Computerized Personal Data Files adopted by a resolution of the General Assembly of the United Nations on the 14th December 1990.

[10]. During 2007 a highly controversial case that has received media attention and caused public debates concerned the collective complaint of the employees of the Commission for the Protection of Competition against their former Chair for subjecting them pervasive workplace surveillance via a monitoring system included CCTV cameras. Other than that, there has been little national debate on data protection or on any deficiencies in effective data protection.. Overall the data protection system is quite effective as there seems to be compliance with the Data Protection Authority's decisions and recommendations. However, there are deficiencies primarily related to the questions of selection of staff and limited funding, which may compromise the independence of the institution and its effective functioning.

# 2. Data Protection Authority

[11]. The institution of the Commissioner for Personal Data Protection was set up by the Processing of Personal Data (Protection of the Individual) Law of 2001[4] as amended[5] and section 106 of the Law on Regulation of Electronic Communications and Postal Services of 2004.[6] The current Commissioner was appointed on 01.03.2002 and her office started operating in May 2002. The appointment is for four years and the current Commissioner is running her second term in office. The legislative framework is based on the Greek model of a single person institution. [7] The role of the Commissioner is to safeguard personal data by protecting personal information relating to an individual against its unauthorised and illegal collection, recording and further use. The law also grants the individual a number of rights, mainly the right of information, the right of access to and the right to object to data collected, as well as the right to submit a complaint to the Data Protection Commissioner on issues pertaining to the application of the Law. The Data Protection Commissioner issues Annual Reports which are posted in her website, containing statistical data on complaints investigated and summaries of activities.

[12]. The Data Protection Commissioner has competence to monitor the implementation of the laws on Processing of Personal Data, as well as all other issues that relate to the protection of the individual in matters

[4] Cyprus/Law No. 138(I)/2001.
[5] Cyprus/Law No. 37(I)/2003.
[6] Cyprus/Law No.112(I)/2004.
[7] See the website of the Commissioner for Personal Data Protection http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_gr/index_gr?OpenDocument (28.01.2009).

of processing of personal data including the relevant articles of the Constitution of the Republic of Cyprus.

[13]. The powers vested in the data protection authority do not meet the requirements of Article 28 of Directive 95/46/EC and are thus insufficient to ensure effective data protection. A detailed examination of each of the powers listed under paragraphs 2-4 of Article 28 of Directive 95/46/EC reveals that only some of these powers are granted to the Cypriot Data Protection Authority, namely the right to be consulted in the preparation of regulations or the adoption of measures, investigative powers, powers of intervention. However the Commissioner was not vested with power to engage in legal proceedings or to bring violations to the attention of judicial authorities.

[14]. In 2005 the European Commission notified the Data Protection Commissioner that there were sections of its Processing of Personal Data Law of 2001 that did not comply with European Data Protection Directive. These included the provisions on the right of information, transfer of data to third countries and procedural mechanisms.[8] The Data Protection Commissioner has drafted amending legislation which purports to bring the law in line with Directive 95/46/EC. At the time of writing, the said draft legislation was being examined by the Ministry of Interior, following which it will be sent to the Law Office of the Republic before sent to Parliament.[9]

[15]. The Processing of Personal Data (Protection of the Individual) Law of 2001[10] as amended[11] provides that the Supervisory authority has the right to consultation in the preparation of regulation or the adoption of measures: "the Council of Ministers, shall on the Commissioner's recommendation, make Regulations for the better implementation of this Law."[12] In terms of investigative powers, powers of intervention, and power to engage in legal proceedings or to bring violations to the attention of judicial authorities the Commissioner has a wide ambit of powers. These include the following:

- The power to "issue directions for the uniform application of provisions concerning the protection of individuals with regard to the processing of personal data".[13]

[8] See http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/9th_annual_report_en.pdf (28.01.2009).
[9] Information provided by the Officer of the Commissioner for Personal Data Protection, Noni Avraam. The researchers have not viewed the proposed amendments.
[10] Cyprus/Law No. 138(I)/2001.
[11] Cyprus/Law No. 37(I)/2003.
[12] Cyprus/Law No. 138(I)/2001, Sec. 27.(1)
[13] Cyprus/Law No. 138(I)/2001, Section 23(a)

- The power to call and assist professional associations and other unions of natural or legal persons which keep filing systems of personal data, in drawing up codes of conduct so as to better protect private life and the rights and fundamental liberties of natural persons in their field of activity.[14]

- The power to submit recommendations and suggestions to controllers or their representatives, if any, and to give, in his discretion, publicity thereto.[15]

- The power to grant the licenses provided by this Law.[16]

- The power to report any violation of the Law to the competent authorities.[17]

- The power to impose the following administrative sanctions:[18]
  (a) warning with a specific time-limit for termination of the contravention;
  (b) a fine of up to £5000 (Euros 8,544);
  (c) temporary revocation of a license;
  (d) permanent revocation of a license;
  (e) the destruction of a filing system or the cessation of processing and the destruction of the relevant data.

- The power to conduct administrative inquiries.[19]

- The power to conduct, on her own initiative or following a complaint, an administrative inquiry on any filing system and, for this purpose, to have access to personal data and collection of any information, including confidential information (except information covered by the confidentiality between advocate and client). Exceptionally, the Commissioner is excluded from access to the particulars of collaborators whose names are kept for reasons of national security or for the detection of particularly serious crimes. [20]

[14] Cyprus/Law No. 138(I)/2001, Section 23(b)
[15] Cyprus/Law No. 138(I)/2001, Section 23(c)
[16] Cyprus/Law No. 138(I)/2001, Section 23(d)
[17] Cyprus/Law No. 138(I)/2001, Section 23(e)
[18] Cyprus/Law No. 138(I)/2001, Sections 23(f) and 25.
[19] Cyprus/Law No. 138(I)/2001, Section 23(g)
[20] Cyprus/Law No. 138(I)/2001, Section 23(h)

- The power to reach a decision on any regulation relating to the processing and protection of personal data.[21]

- The power to issue rules, directions and instruments for the regulation of specific, technical and detailed matters within the ambit of the law.[22]

- The power to draw up annual reports on her activities during the preceding calendar year, which must, inter alia, indicate the necessary legislative amendments that may be required, in the field of protection of individuals with regard to the processing of personal data.[23]

- The power to examine complaints relating to the application of this Law and the protection of the rights of the applicants, when these are affected by the processing of data concerning them, and applications requesting the control and ascertainment of the legality of such processing and to inform the applicants of action taken pursuant to their complaints.[24]

- The power to maintain registers as required by the law.

- The power to co-operate with the corresponding Authorities of other EU Member States of the European Union and the Council of Europe in relation to the exercise of her functions.

[16]. The Commissioner does not have the power to engage in legal proceedings or to bring violations to the attention of judicial authorities.

[17]. During 2006 the Commissioner received 10 applications for transfer of data to third countries and approved six of them. During that year, the Commissioner for Personal Data Protection also received 175 complaints, the bulk of which (46 per cent) concerned spam via e-mail, SMS or fax. Eighty-two per cent of the complaints were directed against the private sector and most of them concerned unsolicited advertising; 10 per cent were directed against the public sector and eight per cent against public law bodies. [25] On 23.05.2007 the

[21] Cyprus/Law No. 138(I)/2001, Section 23(i)
[22] Cyprus/Law No. 138(I)/2001, Section 23(j)
[23] Cyprus/Law No. 138(I)/2001, Section 23(k)
[24] Cyprus/Law No. 138(I)/2001, Section 23(l)
[25] See http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/All/228A250E0D952019C22573A0002B9E53/$file/Annual%20Report%202006.pdf?OpenElement

Commissioner for Personal Data Protection for the first time fined an individual with CYP2000 (Euros 3417) for repeatedly sending advertising messages to a large number of complainants and for ignoring the Commissioner's repeated warnings.

[18]. Regarding the powers of the Commissioner to issue permits for connection and transfer of data, inspect records, investigate complaints, impose sanctions and receive as provided for by the law,[26] the Commissioner has supplied the following statistical data regarding her activities in the last 5 years:

- *Connection Licences:* During 2004 she granted four Connection Licences; during 2005 five Connection Licences; during 2006 five Connection Licences; during 2007 five Connection Licences; and during 2008 nine Connection Licences.

- *Transfer Licences*: During 2003 she granted four Transfer Licences; during 2004 five Transfer Licences; during 2005 five Transfer Licences; during 2006 12 Transfer Licences; during 2007 15 Transfer Licences; and during 2008 ten Transfer Licences.

- *Records inspections*: During 2003 two such inspections were conducted; during 2004 there were five inspections; in 2005 also five inspections; during 2006 there were two inspections; during 2007 there was one inspection; and during 2008 there were two inspections.

- *Complaints investigated*: in 2002 three complaints were received; during 2003 there were 27 complaints received; during 2004, 138 complaints were received; during 2005 there were 172 complaints received; during 2006 there were 179 complaints received; during 2007 there were 241 complaints received; and in 2008, 209 complaints were received.

- *Imposition of administrative sanctions*: in 2004 there were five cases; in 2005 there were three cases; in 2006 there was one case; in 2007 there were four cases; in 2008 there were three cases.

- *Notification of filing systems*[27]: during the years 2001-2003 there were 1370 notifications submitted; in 2004 there were

[26] By sect. 23 of Cyprus/Law 138(I)/2001.

[27] According to section 7(1) of the data protection law (Cyprus/Law No. 138(I)/2001), a controller must notify the Commissioner in writing about the establishment and operation of a filing system or the commencement of processing.

249 notifications; in 2005 there were 108 notifications; in 2006 there were 121 notifications; in 2007 there were 90 notifications; and in 2008 there were 194 notifications submitted. For the year 2008, the sector breakdown is as follows: 110 notifications were submitted from the public sector, 19 notifications from public corporate bodies and 65 from the private sector

[19]. The remit of the data protection authority covers all the main areas in the public and private domain. It covers living natural persons, as well as automated, partially automated, and in some cases, non-automated processing operations, both in the public and the private sectors. The scope of the data protection law also covers the domain of Cypriot law in two instances: (a) by virtue of public international law or (b) by a data controller who is not resident in the Republic, who, for the purpose of processing personal data, has recourse to automated or other means existing in the Republic, unless they were used only for the purpose of transmitting the data through the Republic. However, in order for the Law to be applicable, a data controller resident in the Republic must carry out the processing of personal data. Outside the remit of the law is where the processing of personal data is carried out by a natural person for the exercise of exclusively personal or domestic activities. No other limitations of its remit can be located.

[20]. According to the national data protection legislation[28] the personnel of the office of the Commissioner shall possess the qualifications to be prescribed by Regulations. Such Regulations have not up to now been passed and the officers serving in the office of the Commissioner are civil servants seconded from the Government Department of Information Technology Services and the Department of Public Administration and Personnel. The Office has operated since 1.05.2002 with two officers and four supporting staff; for 2003 there were four officers and five supporting staff. The costs for these years were covered by the budget of the Ministry of Interior. The office had its own budget with the same staff since 2004 with a budget of Cyprus pounds 117,000 (Euros 199,931). In 2005 this was raised to Cyprus Pounds 123,500 (Euros 210,184) with five officers (including one senior officer) and five supporting staff. For 2006 the budget was Euros 221,000 with the same staff levels as 2005. For 2007 the budget was Euros 245,800 for six officers and six supporting staff. For 2008 the budget was Euros 303,000 for six permanent officers and seven supporting staff (two computer officers and four in secretarial posts).[29] The Commissioner's Annual report for 2006 refers to the problem of

[28] Cyprus/Law No. 138(I)/2001, Section 22(1).
[29] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).

under-staffing of the Commissioner's office which inevitably results in the inadequate execution of its tasks, a fact commented upon by the Schengen Evaluation Committee as affecting also the impartiality of the institution. The Commissioner herself, in her letter to the researchers dated 02.02.2009, states that the fact that her staff consists of public servants in whose recruitment she is not involved, is a factor that affects the independence and effective functioning of the institution. It had always been the demand of the Commissioner since the establishment of the institution, also adopted by the Schengen Evaluation on the capacity of Cyprus to implement the Schengen acquis during the evaluation on personal data, to set up positions specifically for the Office of the Commissioner for Personal Data Protection; however this demand was not accepted.[30]

[21]. The Law provides for the independence of the Commissioner by stating that "in the exercise of his duties, the Commissioner shall act according to his conscience and in accordance with the law" and "shall be subject to a duty of confidentiality, which shall continue to exist even after he ceases to be the Commissioner." [31] Moreover, it provides that "as a witness or expert witness he may only give [advice or testimony] on matters which relate to the compliance by the controllers with the provisions of this Law."[32] Apart from the staffing issues referred to above no concerns have been raised by the Commissioner as to the independence of the data protection authority. Also, in the researchers' opinion, the overall functioning of the institution does not raise concerns regarding its impartiality or independence.

[22]. The mandate of the Commissioner for Personal Data Protection is provided in th**e** Law on Processing of Personal Data N.138(I)/2001, as amended by Law N.37(I)/2003. The law prohibits the collection and processing of sensitive personal data and lists the circumstances under which this is exceptionally allowed. Under article 6(3) of Law 138(I)/2001, the Council of Ministers may issue regulations following a proposal by the Personal Commissioner for Personal Data Protection, on the processing of data in cases other than the ones provided for under the law when there are serious reasons of public interest involved. The Law regulating Electronic Communication and Postal Services N.112(I)/2004 that purports to transpose inter alia Directive 2002/58/EC regulates the secrecy of communications and

[30] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).

[31] Cyprus/Law No. 138(I)/2001, Section 27(1).

[32] Section 21.(1), Cyprus/Law on Data Protection 2001. The reference of art. 28 of the Directive require that "these authorities shall act with complete independence in exercising the functions entrusted to them."

the use of traffic and location data, telephone directories and unsolicited communications. Moreover, it complements the provisions of the Law for the Processing of Personal Data and provides for the protection of the legitimate interests of subscribers of electronic communications networks and services who are legal persons. Section 98 of the Law provides for the appropriate technical and organizational measures to be taken by providers of publicly available electronic communications services and networks to safeguard the security of their services and networks. Section 99 provides for the confidentiality of the communications and related traffic data. With regard to traffic data, Section 100 provides that such data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. The data protection authority is quite proactive and has become active on its own initiative with investigations and audits. Its decisions and/or opinions are readily available to the public: a summary of the main decisions is included in the Annual Reports published on the Commissioner' website and the full decisions, save for the details of the complainants, can be made available on request.

[23]. On 23.11.2001 the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981 was transferred into national law through Ratifying Law N. 28(III)/2001. On 4.7.2003 the Additional Protocol of the said Convention was transferred into national law through ratifying Law N. 30(III)/2003.

[24]. The monitoring role of the data protection authority in Cyprus is well practiced. Violations of data protection legislation (especially information duties) are detected via complaints by individuals, media exposure and via self-initiated investigations of the data protection authority. The data protection authority often acts proactively as it takes up any information that is in the public domain or that comes to the authority's attention through the media or otherwise in order to commence an investigation.

[25]. According to the Commissioner the Opinions of the Working Party of Article 29 of Directive 95/46 are "the guidelines for the data protection" and are described as "useful tools in the interpretation and/or better implementation of the law". [33]

[26]. The data protection authority performs a multifaceted advisory role as provided by the law; it is empowered to call and assist professional

[33] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).

associations and other unions of natural or legal persons which keep filing systems of personal data, in drawing up codes of conduct so as to better protect private life and the rights and fundamental liberties of natural persons in their field of activity.[34] Also the data protection authority is empowered to make recommendations and regulations for the better implementation of this Law.[35] In practice the data protection authority participates in law-making commissions that contain provisions relevant to the collection and processing of personal data and participates in meetings of the various Parliamentary Committees during the debate of the relevant legislation.[36]

[27]. Since 2002, the data protection authority has been involved in various awareness raising activities such as number of press conferences, open seminars to the public, as well as lectures by officers of the authority to organisations in the public as well as the private sector. In 2005, 2006 and 2007 the Office engaged in numerous public awareness efforts, organising seminars on the rights of data subjects and on the lawful use of personal data and workplace monitoring. In addition, officers of the authority delivered presentations to various governmental departments, including the Police Academy, and also issued informational statements to the media and the University of Cyprus. Also the data protection authority has published and disseminated booklets informing the public of data protection rights and obligations and providing guidelines. The leaflets, which are also available also on its website, provides information on how personal data can be protected during use of the internet and recommends that data controllers create websites that comply with data protection rules. Another booklet includes guidelines about the lawful use of video surveillance cameras, whilst a third one that was circulated in schools contains information on personal data and the internet.

# 3. Compliance

[28]. We are informed by the data protection authority that in general there is a good record of compliance with the recommendations of the authority. The authority advises that a random check they carried out showed that the majority of recommendations issued are immediately complied with by controllers. However, due to staff shortages, the

[34] Under sect. 23(c) of Cyprus/Law No. 138(I)/2001.
[35] Cyprus/Law No. 138(I)/2001, Sec. 27.(1).
[36] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).

authority does not have the capacity to check compliance on every instance for which it has issued a recommendation.[37]

[29]. The procedures for registration with the data protection Commissioner of organisations processing personal data are set out by section 7(2) of the Law[38] and are undertaken through the submission of a relevant form of notification under this section of the law.

[30]. Although prohibited as a rule under Section 6(1) of the Law[39], the processing of sensitive data is permitted under sections 6(2) and 6(3) which list a number of circumstances under which the processing of sensitive data is allowed. These include processing which is necessary so that the controller may fulfil his obligations or carry out his duties in the field of employment law (section 6(2)(b) of the Law).

[31]. According to the data protection Commissioner, the majority of organisations comply with the requirement for the submission of notification under section 7 of the law. However, the Commissioner is of the view that in terms of the provision of section 6(2)(b) of the Law, compliance particularly in the public sector "is not satisfactory since very few organisations have applied for and have been given licence at this stage to process sensitive data in order to carry out their duties in the field of employment law".[40] Trade unions do not have a role in regularly monitoring data protection in employment. The only instance where a trade union was involved was that of the union of public servants, which took the initiative to publicise and complain about personal data violation in the Commission for the Protection of Competition, as detailed in paragraph 37 below.

[32]. Each organisation is responsible for designating the procedures for the appointment of data protection officers or similar persons with a special expertise and special awareness raising role within private and public organisations. The Commissioner advises that "most of the large private institutions have designated such officers" and that the level of compliance with the law is to a large extent detected from the data provided in the notifications of their respective filing systems. However, the Commissioner advises that the monitoring of compliance on a statistical yearly basis is impossible given the under-staffing of her office. The currently used procedure for monitoring compliance with the legislation comprises of examining the

[37] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).

[38] Cyprus/Law No. 138(I)/2001.
[39] Cyprus/Law No. 138(I)/2001.
[40] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).

notifications submitted to the Commissioner by the controllers and through the regular exchange of correspondence with controllers, often requiring clarification and/or recommendations on data processing and the investigation of filing systems maintained by controllers. [41]

# 4. Sanctions, Compensation and Legal Consequences

[33]. Under section 25(1) of Law No. 138(I)/2001, the Commissioner may impose on the controllers or their representatives, the following administrative sanctions in case of contravention of their obligations which arise from this Law and from every other regulation concerning the protection of individuals with regard to the processing of personal data:

- (a) a warning with a specific time-limit for termination of the contravention;
- (b) a fine of up to £5000;
- (c) temporary revocation of a license;
- (d) permanent revocation of a license;
- (e) the destruction of a filing system or the cessation of processing and the destruction of the relevant data.

[34]. The law provides that, with the exception of the warning, the above administrative sanctions will be imposed following a hearing with the controller or his representative and that they shall be proportionate to the seriousness of the relevant contravention (section 25(2) of Law No. 138(I)/2001).

[35]. After being sanctioned, the controllers may either comply with the sanction within a short period of time or alternatively may dispute the decision of the Commissioner within 75 day by applying to the Supreme Court to set aside the decision via the general challenge of administrative action in accordance with Article 146 of the Constitution. If the matter carries a fine, then the officer in charge of

[41] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).

processing must pay forthwith, otherwise the matter will be referred to the District Court. Following compliance such as the submission of the relevant forms containing the data to the Commissioner or on spot inspection to ensure execution of the sanction such as the destruction of documents in the presence of a representative of the data protection authority.

[36]. In addition to the aforementioned sanctions imposed by the Commissioner, Law No. 138(I)/2001 creates the following offences which carry different penalties depending on the perpetrator's motive. In particular, offences are committed where a person:

(a). Omits to notify the Commissioner of the establishment and operation of a filing system, the carrying out of the processing or any change in the terms and conditions for the grant of a license;

(b). Maintains a filing system without a license or in contravention of the terms and conditions of the license granted by the Commissioner;

(c). Proceeds to the combination of filing systems without notifying the Commissioner;

(d). Makes a combination of filing systems without a license issued by the Commissioner, where such a license is required, or in contravention of the terms of the license already granted to him;

(e). Without being entitled to do so, intervenes in any way in a filing system of personal data or acquires knowledge thereof, or removes, alters, damages, destroys, processes, transmits, communicates the data, or renders them accessible to persons not entitled to access or permits such persons to acquire knowledge of the said data or makes use of them in any way;

(f). Being a controller, does not comply with the provisions of this Law during the processing;

(g). Being a controller, does not comply with the decisions of the Commissioner for the exercise of the right of access, the right of objection or the imposition of the administrative sanctions;

(h). Being a controller, transmits personal data in violation of the law, or being a controller does not comply with a decision of the Court.

Where the aforesaid acts were intended to obtain for himself or anyone else an unlawful financial benefit or cause injury to a third party, the person found guilty is liable to imprisonment for a term not exceeding five years and/or to a fine not exceeding five thousand pounds (Euros 8,544)

Where the aforesaid acts endanger the free functioning of the government or national security, the person found guilty shall be liable to imprisonment for a term not exceeding five years and/or to a fine not exceeding five thousand pounds (Euros 8,544).

If the aforesaid acts were caused by negligence, the person found guilty shall be liable to imprisonment for a term not exceeding three years and/or to a fine not exceeding three thousand pounds (Euros 5,126).

The offences committed in contravention of the provisions of this section for which no other penalty is provided, are punishable with imprisonment for a term not exceeding one year and/or with a fine not exceeding two thousand pounds (Euros 3,417).

[37]. Article 17 of the national data protection legislation[42] provides that the controller shall compensate a data subject who has suffered damage by reason of violation of any provision of this Law, unless he proves that he is not responsible for the event that caused the damage

[38]. To some extent the enforcement of data protection legislation through sanctions and/or compensation payments depends largely on personal initiative of data subjects but not entirely: the data protection authority has been involved in self-initiated investigations and has taken up cases from the media. Data subjects are certainly more informed and assisted by the data protection authority via legal advice and consultation than they were before the establishment of the data protection authority. However, no legal representation in court proceedings is offered and there are no NGOs who can assist in theory or in practice operative in Cyprus. There is no legal assistance and representation in data protection cases institutionalised (publicly funded NGOs or associations, public bodies performing this function etc.). The financial risk of legal procedures in data protection cases such as court fees, fees of attorney etc. are borne by the data subject.

[39]. In July 2007 a well-known case that attracted considerable media attention involved the collective complaint of the entire staff of the office of the Cypriot Commission for the Protection of Competition (CPC). The staff, which eventually went on strike with the support of the public employees' trade union, protested at being subjected to pervasive workplace surveillance by the CPC's chairman via a monitoring system which included CCTV cameras, microphones throughout the offices, including restrooms, which could be remote-accessed through the personal computer of CPC's chairman. Moreover, the employees claimed that their emails and telephone

[42] Cyprus/Law No. 138(I)/2001.

conversations were tapped. The Cypriot police investigated their claim for breach of privacy; however, the chairman of CPC denied some of these claims, countering that the system was not secret and was necessary to keep his employees on task. The Report of Privacy International on Cyprus states that "in their ongoing investigation, the police accessed the commissioner's computer and discovered about 600 pictures, freeze-frames from video recordings, including some 400 of a particular female employee." The data protection Commissioner stated that the CPC should have notified her office of the monitoring system, but failed to do so. Also, the Data Protection Commissioner noted that since the CPC surveillance scandal broke, her office received numerous similar complaints from across the country. [43] The investigation of this case by the data protection commissioner continues. [44]

[40]. The data protection authority is not aware of any cases involving compensation for a victim of violation of data protection rights. [45]

# 5. Rights Awareness

[41]. There are no other studies and/or surveys on awareness regarding data protection law and rights in the population and/or in special segments of society (companies, legal practitioners, employers, civil servants etc.) other than the two Eurobarometer surveys on data protection.[46]

# 6. Analysis of deficiencies

[42]. The main deficiencies regarding effective data protection and effective relevant bodies/institutions concern the appointment of the staff of the Commissioner's office as well as the difficulties faced in cases of non-cooperation by a controller or a third party during the investigation of complaints or self-initiated investigations by the data protection Commissioner. The data protection authority has proposed amendments to the law addressing this gap.[47]

[43] See http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559499 accessed 30.1.2009.
[44] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).
[45] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).
[46] carried out in 2008 available at http://ec.europa.eu/justice_home/fsj/privacy/news/index_en.htm
[47] Letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002). The researchers have not seen the proposed amendments.

[43]. The data protection law covers all main areas in the public and private domain with the general prohibition of "collection and processing of sensitive data". However there are areas that are exempted/ excluded from protection, for which "the collection and processing of sensitive data is permitted, when one or more of the following conditions are fulfilled":

- The data subject has given his explicit consent, unless such consent has been obtained illegally or is contrary to accepted moral values or a specific law provides that consent does not lift the prohibition. [48]

- Processing is necessary so that the controller may fulfil his obligations or carry out his duties in the field of employment law.

- Processing is necessary so that the controller may fulfil his obligations or carry out his duties in the field of employment law;

- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.[49]

- Processing is carried out by a foundation, association or other non-profit-making organisation which has political, philosophical, religious or trade-union aims, and relates solely to its members and such other persons with whom the said association, foundation or organisation retains relations by reason of its purposes. Such data may be communicated to third parties only if the data subject gives his consent.[50]

- The processing relates solely to data which are made public by the data subject or are necessary for the establishment, exercise or defence of legal claims before the Court.[51]

- The processing relates to medical data and is performed by a person providing health services by profession and has a duty of confidentiality or is subject to relevant codes of conduct, on condition that the processing is necessary for the purposes of

[48]Cyprus/Law No. 138(I)/2001, Section 6.(2)(a).
[49] Cyprus/Law No. 138(I)/2001, Section 6.(2)(b).
[50] Cyprus/Law No. 138(I)/2001, Section 6.(2)(c).
[51] Cyprus/Law No. 138(I)/2001, Section 6.(2)(d).

preventive medicine, medical diagnosis, the provision of care or the management of health-care services. [52]

- Processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent. [53]

- Processing is necessary for the purposes of national needs or national security, as well as criminal and reform policy, and is performed by a service of the Republic or an Organisation or Foundation authorized for this purpose by a service of the Republic and relates to the detection of crimes, criminal convictions, security measures and investigation of mass destructions.[54]

- Processing is necessary for the purposes of national needs or national security, as well as criminal and reform policy, and is performed by a service of the Republic or an Organisation or Foundation authorized for this purpose by a service of the Republic and relates to the detection of crimes, criminal convictions, security measures and investigation of mass destructions. [55]

- Processing is performed solely for statistical, research, scientific and historical purposes, on condition that all the necessary measures are taken for the protection of the data subjects. [56]

- Processing is performed solely for journalistic purposes or in the framework of artistic expression and as long as the right to privacy and family life is not violated. [57]

- Moreover, the Council of Ministers may on the Commissioner's recommendation, issue regulations for the processing of sensitive data, in cases other than those referred to in subsection (2) when serious matters of public interest concur. [58]

[44]. We have not been provided with the proposed amendments to the legislation to express an opinion as to whether the deficiencies can be

[52] Cyprus/Law No. 138(I)/2001, Section 6.(2)(e).
[53]Cyprus/Law No. 138(I)/2001, Section 6.(2)(f).
[54] Cyprus/Law No. 138(I)/2001, Section 6.(2)(f).
[55] Cyprus/Law No. 138(I)/2001,Section 6.(2)(g).
[56] Cyprus/Law No. 138(I)/2001, Section 6.(2)(h).
[57]Cyprus/Law No. 138(I)/2001, Section 6.(2)(i).
[58] Cyprus/Law No. 138(I)/2001, Section 6.(3).

filled or reduced by new or amended legislation. However, we are assured that the proposed amendments cover the gaps. There is certainly an issue of resource allocation as the data protection authority is understaffed and under-resourced. Moreover, in spite of the awareness raising and the training offered, a great deal more can be done to ensure better knowledge and better implementation of EU legislation and the international standards relevant for data protection and/or better application of existing legislation.

# 7. Good Practice

[45]. There a number of websites that make available information regarding data protection (also in English), including the website of the Cypriot data protection authority[59] as well as the website of the Privacy International, which as an entry on Cyprus.[60]

[46]. No good practice can be located or pointed out by any of the involved parties.[61]

# 8. Miscellaneous

[47]. In July 2008 the Commissioner for the Protection of Personal Data has issued her Annual Report for 2007 which will be uploaded on her website in the near future. The report contains statistical data on notifications submitted to the Commissioner for the keeping and processing of data (36 from the public sector; 52 from the private sector and two from legal persons of public law, total 90 notifications). Statistical data is offered also on the number of complaints received annually since 2003 and the categories of complaints which are as follows: Spam messages mainly to mobile phones (110 complaints, 50 per cent of all complaints); closed circuit video cameras (21 complaints, 9.5 per cent); discovery of personal

[59] At http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument (28.01.2009)

[60] Last entry 18.12.2007. Accessed on 20.1.2009, see http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-559499#[20].

[61] Not even the Data Protection Authority is aware of any good practises as confirmed by the letter to researchers by the Commissioner for Personal Data Protection 2.2.2009 (File No. 04.01.002).

data mainly through the press (27 complaints, 12 per cent); and 16 complaints (7 per cent) alleged that the principle of proportionality had been violated by insurance companies which required their customers to submit the results of medical tests. The vast majority of complaints were directed against the private sector (82%) given the high number of complaints regarding unwanted advertisements. A total of 220 complaints were received in 2007, out of which 85 were investigated. The reason for not investigating a larger number is the difficulties in investigating Spam messages. Out of the 85 cases decided, 20 were found to be well founded and the accused complied; an administrative sanction was imposed in one case; the investigation was interrupted due to satisfaction of the complainant in three cases; the investigation was interrupted due to lack of evidence in 16 cases; the investigation was interrupted due to lack of jurisdiction in 17 cases; one complaint was withdrawn by the complainant; and 25 complaints were found to be unfounded. One of the well founded complaints concerned the use by a local authority of a system of fingertips to monitor the arrival and departure of personnel, where the accused complied with the Commissioner's decision and removed this system. On the issue of medical tests required by insurance companies, the Commissioner found that insurance companies have the right to request such data only when absolutely necessary in order to determine the amount of compensation and not as a matter of routine practice. The Commissioner also found that the principle of proportionality was violated: by the Births Registration department which required parents to fill out a form asking for unnecessary data such as the date of marriage of parents, whether it is their first marriage, etc; by the Ministry of Education in the School Leaving certificates which have since been revised; and many more similar cases.

[48]. The specifications of a new system of street cameras, as set out in the terms of the relevant public procurement, provide that the system must record on video all vehicles and pedestrians crossing the points controlled by the cameras, irrespective of whether any traffic or other offence has been committed. Four years ago, an effort was made to legalise the use of such cameras, but the said bill did not meet with the approval of the House of Parliament. The Cypriot Commissioner for the Protection of Personal Data stated that the current legislation forbids the use of such cameras, whilst the chairman of the Parliamentary Committee of Legal Affairs stated that such a system may violate the constitutional right to private life. The Ministry of Transport and Public Works who issued the said procurement sought to justify the insertion of such term in the public procurement notice as an effort to record vandalising incidents of the cameras with sprays or otherwise, as it happened in the past with the conventional street cameras, adding that the video will only be retained for 24 hours and

will then be erased. The Ministry added that it will only make use of such system if the current law is amended so as to allow it. However, the decision of the Ministry to call for tenders on the basis of these specifications before the issue is discussed in Parliament is likely to cause problems, because by the time the matter is brought before the House the tenderers will already have submitted their tenders on the basis of the specifications issued, which provide for the video-recording of all activities. Several dozens of companies, including joint ventures between Cypriot and foreign firms, have expressed interest in the procurement. The deadline for the submission of the tenders was 03.10.2008

# Annexes

## Annex 1 - Tables and Statistics

Please complete the table below

| | 2000[62] | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 |
|---|---|---|---|---|---|---|---|---|
| Budget of data protection authority | N/a | N/a | No separate budget. Part of the budget of the Interior Ministry | No separate budget. Part of the budget of the Interior Ministry | Cyprus pounds 117,000 (Euros 199,931) | Cyprus Pounds 123,500 (Euros 210,184) | Euros 221,000 | Euros 245,800 |
| Staff of data protection authority | N/a | N/a | 6 (2 officers and 4 supporting staff) | 9 (4 officers and 5 supporting staff) | 9 (4 officers and 5 supporting staff) | 10 (5 officers including one senior officer and 5 supporting staff) | 10 (5 officers including one senior officer and 5 supporting staff) | 12 (6 officers and 6 supporting staff) |

[62] The Commissioner was appointed in 2002. Prior to this date, the institution did not exist.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative<br><br>There is no separate record of self initiated procedures | N/a | N/a | | | | | | |
| Number of data protection registrations | N/a | N/a | | | | | | |
| Number of data protection approval procedures<br><br>Please see additional cells below | N/a | N/a | | | | | | |
| Number of complaints received by data protection authority | N/a | N/a | 3 | 27 | 138 | 172 | 179 | 241 |
| Number of complaints upheld by data protection authority<br><br>The Commissioner's office does not classify complaints according to whether they were | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| upheld or not. In order to obtain this information, they would have to check each and every decision. They informed us that they do not have the manpower to carry out such a time-consuming task. | | | | | | | | |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Follow up activities of data protection authority, once problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)<br><br>The data protection authority has advised that the statistical monitoring of compliance activities per year is not possible. | | | | | | | | |
| 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)<br><br>The figures shown represent sanctions imposed by the Data Protection Commissioner. There is no record of sanctions imposed by the Court. There are no other authorities dealing with the implementation of the data protection laws. | N/a | N/a | 0 | 0 | 5 | 3 | 1 | 4 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/compensation)<br><br>The Commissioner's office does not classify sanctions according to type and this information is therefore not available. | | | | | | | | |

Any other tables or statistics relevant for assessment of effectiveness of data protection, where available

| Type of Procedure | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 |
|---|---|---|---|---|---|---|
| Notifications of filing systems submitted to the data protection commissioner | 1370 (from 2001-2003) | 249 | 108 | 121 | 90 | 126(until October 2008) |
| Issue of connection permits | 0 | 4 | 5 | 5 | 5 | 9 |
| Issue of permits transfer data to third countries | 4 | 5 | 5 | 12 | 15 | 10 |
| Checks on data records | 2 | 5 | 5 | 2 | 1 | 2 |

# Annex 2 – Case Law

Please present at least 5 cases on data protection from courts, tribunals, data protection authorities etc. (criteria of choice: publicity, citation in media, citation in commentaries and legal literature, important sanctions) in your country, if available (please state it clearly, if less than 5 cases are available)

| | |
|---|---|
| **Case title** | Paphos Chief of Police v. Billai Ali, Mubasher Nawaz and Numan Ahmed Miah |
| **Decision date** | 08.07.2008 |
| **Reference details** (reference number; type and title of court/body; in original language and English [official translation, if available]) | Case No. 6986/2008<br>Court decision<br>Επαρχιακό Δικαστήριο Πάφου<br>District Court of Paphos |
| **Key facts of the case** (max. 500 chars) | The accused in this case pleaded guilty to the charge of ,inter alia, forging credit cards by inserting other people's personal data on the magnetic stripe and using them in shops in order to obtain goods whilst charging the accounts of other persons, in contravention of the data protection legislation |
| **Main reasoning/argumentation** (max. 500 chars) | The Court found the access to personal data which the accused managed to obtained through the use of technology, as well as the use of such data by criminal elements as "frightening", particularly where such data is related to the financial activities of the subject of the data, adding that this new form of crime affects and invades the personal and private life and freedom of the person. |
| **Key issues (concepts, interpretations) clarified by the case** (max. 500 chars) | In the course of imposing a sentence, the Courts must take into consideration the seriousness of the crime committed, the increasing trends of committing a particular offence and the personal circumstances of the accused. However, the latter consideration must not be allowed to neutralise the preventing effect of the sentence, both on the accused themselves, in order to stop the offenders from repeating the same offence in the future, as well as to prevent the commission of the same offence by others. |
| **Results (sanctions) and key consequences or implications of the case** (max. 500 chars) | A number of concurrent prison sentences were imposed, the longest one being 20 months. The sentence takes into consideration a number of mitigating factors, such as the accused person's young age, their personal circumstances, their clean record and their willingness to confess and cooperate with the people. It is nevertheless a harsh sentence, based rather on the judge's intention of it serving as a deterrent for other potential perpetrators. The national origin of the perpetrators did play a role in the judge's reasoning, who expressed his "concern" over the fact that "foreign persons visit Cyprus with the sole purpose of [pursuing] criminal aims". |

| | |
|---|---|
| **Proposal of key words for data base** | Credit card fraud, access to personal data |

| | |
|---|---|
| **Case title** | Decision under section 23 (11) of the Law on Processing of Personal Data (Protection of the Person) of 2001 |
| **Decision date** | 26.02.2004 |
| **Reference details** (reference number; type and title of court/body; in original language and English [official translation, if available]) | Επίτροπος Προστασίας Προσωπικών Δεδομένων<br>Commissioner for the Protection of Personal Data |
| **Key facts of the case** (max. 500 chars) | A complaint was submitted to the Personal Data Commissioner regarding the actions of the anti-drug squad of the police at the Larnaca airport, who made copies of the passport of the complainant and obtained and recorded information from it regarding the complainant and his parents in contravention of the data protection law, based on a suspicion that he may have been carrying drugs. In the end no evidence was found against the complainant for any drug related or other offence. In response to a letter from the data protection commissioner, the chief of police admitted that the complainant was investigated because he was deemed, through the profiling method, to be a suspect for drug related offences and as such the actions of the anti-drug squad were lawful and justified in accordance with section 12(4) of the law, which allows the processing of personal data for the purposes of prevention, investigation, detection and prosecution of criminal offences.[63] |

[63] Article 12(4) of the law reads: "By a decision of the Commissioner, on application by the controller, the obligation to inform under subsectior personal data is performed for …the prevention, investigation, detection and prosecution of criminal offences."

| | |
|---|---|
| **Main reasoning/argumentation** (max. 500 chars) | The Commissioner pointed out that Section 12(4) of the law was irrelevant as it concerned the waiving of the obligation to inform the data subject about the processing of his personal data. The Commissioner accepts that the police hs the power to search persons arriving from abroad if there is information about that person's potential involvement in crime, however in the case of the complainant the search did not reveal any evidence against him. With reference to section 4(1)(c) of the law, which requires that the data collected must be relevant, appropriate and not excessive in relation to the purposes of processing, the Commissioner found that the action of the police to photocopy and archive the complainant's passport after no incriminating evidence emerged against him and the processing of data relating to the complainant's parents was a violation of section 4(1)(c) of the law. |
| **Key issues (concepts, interpretations) clarified by the case** (max. 500 chars) | The Commissioner clarified that once the search of a suspect does not bring to light any incriminating evidence, then the collection and archiving of that person's personal data, and particularly of the data of third persons (his parents) contravenes the provision of the law which requires data "relevant, appropriate and not excessive" (article 4(1)(c)). |
| **Results (sanctions) and key consequences or implications of the case** (max. 500 chars) | The Commissioner ordered the police to destroy the personal data so collected and to inform the Commissioner about the measures taken to this end. Although no information is available as to whether the police has effectively complied with this decision, there are several instances where members of the police force, particularly at the airport, who show a lack of knowledge of the data protection principles. The Commissioner's limited mandate does not leave margin for any other actions but it is obvious that more far reaching measures, like a code of conduct for the police or awareness raising measures, are required. |
| **Proposal of key words for data base** | Police suspect, photocopy passport, excessive data. |

Below is the original text of the decision:

## Απόφαση με βάση το άρθρο 23(ιβ) του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001

## Γεγονότα:

1. Στις 9 Σεπτεμβρίου 2003 εστάλη στον Έντιμο Υπουργό Δικαιοσύνης και Δημοσίας Τάξεως επιστολή από τον M.Z. στην οποία αναφέρονται ορισμένα γεγονότα που κατ' ισχυρισμό του συνέβησαν στο Αεροδρόμιο Λάρνακας κατά την επιστροφή του από το εξωτερικό.

   Αντίγραφο της πιο πάνω επιστολής απεστάλη και σ' εμένα.

2. Στην επιστολή γίνεται αναφορά στη συμπεριφορά ανδρών της Υ.ΚΑ.Ν., καθώς και στο ότι, σύμφωνα πάντα με τους ισχυρισμούς του παραπονούμενου, ελήφθη φωτοαντίγραφο του διαβατηρίου του και πληροφορίες για το άτομό του και τους γονείς του, κατά παράβαση του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001, που στο εξής θα αναφέρεται ως Νόμος.

1. Με βάση τις εξουσίες που μου χορηγούνται από το άρθρο 23(ιβ) του Νόμου, προχώρησα στην εξέταση του μέρους του παραπόνου που αναφέρεται στη συλλογή/επεξεργασία προσωπικών δεδομένων.

2. Στις 20 Οκτωβρίου 2003 απέστειλα επιστολή στον Υπουργό Δικαιοσύνης και Δημοσίας Τάξεως και στον Αρχηγό Αστυνομίας, ζητώντας τις απόψεις τους σε σχέση με τους ισχυρισμούς του παραπονούμενου.

3. Ο Αρχηγός Αστυνομίας με επιστολή του ημερομηνίας 24 Νοεμβρίου 2003 επισύναψε αντίγραφο επιστολής του Υπεύθυνου Υ.ΚΑ.Ν. Λάρνακας, στην οποία γίνεται αναφορά μόνο στις συνθήκες έρευνας, τόσο των αποσκευών όσο και του ίδιου του παραπονούμενου.

   Στην δεύτερη επιστολή αναφέρεται ότι μετά τις πιο πάνω έρευνες δεν «ανεβρέθηκε οτιδήποτε ύποπτο».

   Αξίζει να σημειωθεί ότι, στην ίδια επιστολή αναφέρεται ότι ο παραπονούμενος «κρίθηκε ύποπτος για μεταφορά ναρκωτικών με τη μέθοδο του PROFILE, όπως γίνεται σε αρκετά αεροδρόμια της Ευρώπης».

4. Στην επιστολή του της 24ης Νοεμβρίου 2003, ο Αρχηγός Αστυνομίας εκφράζει τη γνώμη ότι «οι ενέργειες των μελών της Υ.ΚΑ.Ν. ήταν καθόλου νόμιμες γιατί έγιναν για σκοπούς πρόληψης, διερεύνησης, διακρίβωσης ποινικών αδικημάτων όπως προβλέπει το άρθρο 12(4) του Νόμου».

5. Με επιστολή του με ημερομηνία 15 Δεκεμβρίου 2003, ο Γενικός Διευθυντή του Υπουργείου Δικαιοσύνης και Δημοσίας Τάξεως απάντησε στην επιστολή μου της 20ης Οκτωβρίου 2003, εκθέτοντας στην ουσία τις θέσεις του Αρχηγού Αστυνομίας, όπως αυτές περιλαμβάνονται στην επιστολή του υπεύθυνου της Υ.ΚΑ.Ν. Λάρνακας, που αναφέρεται στην παρ. 5.

   Επειδή όπως προέκυψε από την σχετική αλληλογραφία, το Υπουργείο Δικαιοσύνης και Δημοσίας Τάξεως δεν είχε άμεση γνώση των γεγονότων, αλλά ενημερώνετο για την υπόθεση από τον Αρχηγό Αστυνομίας, οι επόμενες ενέργειές μου απευθύνονταν μόνο προς τον Αρχηγό Αστυνομίας.

6. Με μεταγενέστερη επιστολή μου προς τον Αρχηγό Αστυνομίας ημερομηνίας 3 Δεκεμβρίου 2003, διευκρίνισα ότι η εξέταση που διενεργούσα αφορούσε το μέρος του παραπόνου που σχετίζετο με τη συλλογή και επεξεργασία προσωπικών δεδομένων και όχι τη μέθοδο και τον τρόπο διεξαγωγής της σωματικής και άλλης έρευνας.

   Πρόσθετα επίσης ότι η αναφορά στο άρθρο 12(4) του Νόμου ήταν άσχετη με την υπό εξέταση υπόθεση, γιατί το εδάφιο αυτό αφορά την άρση της υποχρέωσης πληροφόρησης των υποκειμένων των δεδομένων.

   Με την επιστολή μου αυτή είχα καλέσει τον Αρχηγό Αστυνομίας να υποβάλει τις θέσεις του ή οποιεσδήποτε διευκρινήσεις είτε γραπτώς ή προφορικά.

7. Επειδή δεν είχα οποιαδήποτε απάντηση στην επιστολή μου της 3ης Δεκεμβρίου 2003, στις 7 Ιανουαρίου 2004 απέστειλα δεύτερη επιστολή στον Αρχηγό της Αστυνομίας στην οποία ανάφερα ότι δεδομένου ότι δεν απάντησαν στην επιστολή μου, θεωρούσα ότι δεν είχαν τίποτε να προσθέσουν ή διευκρινίσουν και ότι δεν αμφισβητούσαν τα γεγονότα σχετικά με την συλλογή και επεξεργασία των προσωπικών δεδομένων όπως τα εξέθεσε στην επιστολή του ο παραπονούμενος.

8. Και σε αυτή την επιστολή δεν είχα μέχρι σήμερα οποιαδήποτε απάντηση.

   Επειδή θεωρώ ότι δεν δικαιολογείται πλέον οποιαδήποτε περαιτέρω καθυστέρηση στην διεκπεραίωση και συμπλήρωση της εξέτασης του παραπόνου, θα προχωρήσω στην έκδοση της σχετικής Απόφασης.

Δεν εξετάζω το μέρος του παραπόνου του M.Z. που αναφέρεται στις συνθήκες και τον τρόπο διεξαγωγής σωματικής έρευνας από άνδρες της Υ.ΚΑ.Ν. κατά την επιστροφή του από το εξωτερικό, γιατί αυτό δεν αφορά συλλογή και επεξεργασία προσωπικών δεδομένων.

Η εξέταση του παραπόνου περιορίζεται στους ισχυρισμούς που αφορούν τη συλλογή προσωπικών δεδομένων με τη φωτοτύπηση του διαβατηρίου του παραπονούμενου και με την παροχή από αυτό πληροφοριών για τους γονείς του, οι οποίες στη συνέχεια καταγράφηκαν/ καταχωρήθηκαν σε αστυνομικό αρχείο, κατά παράβαση του Νόμου.

Κατά την άσκηση των εξουσιών της για καταπολέμηση της εμπορίας, διακίνησης και χρήσης ναρκωτικών η Αστυνομία/ Υ.ΚΑ.Ν. έχει εξουσία να ερευνά οποιοδήποτε πρόσωπο το οποίο αφικνείται από το εξωτερικό αν έχει πληροφορίες για πιθανή εμπλοκή του ή στα πλαίσια του συνήθους ελέγχου, ή ελέγχου που γίνεται με τη μέθοδο PROFILE.

Στην υπό εξέταση περίπτωση, μετά από τη διενέργεια σωματικής έρευνας του παραπονούμενου και έρευνα των αποσκευών του κατά την άφιξή του στο αεροδρόμιο Λάρνακας, η Υ.ΚΑ.Ν. αναφέρει, στην επιστολή του υπεύθυνου της στη Λάρνακα, ότι δεν προέκυψε οτιδήποτε ύποπτο.

Αφού έλαβα υπόψη τις βασικές προϋποθέσεις για τη νομιμότητα της επεξεργασίας προσωπικών δεδομένων, όπως αυτές εκτίθενται στο άρθρο 4(1) του Νόμου και ιδιαίτερα την παράγραφο (γ), η οποία ορίζει ότι τα δεδομένα που συλλέγονται πρέπει να είναι συναφή, πρόσφορα και όχι περισσότερα από ότι κάθε φορά απαιτείται εν όψει των σκοπών της επεξεργασίας και αφού θεωρώ ως αληθείς τους ισχυρισμούς του παραπονούμενου για τη συλλογή και επεξεργασία τόσο δικών του προσωπικών δεδομένων όσο και τρίτων (των γονιών του), έχω καταλήξει στα εξής:

- Μετά τη διαπίστωση ότι από τα αποτελέσματα της έρευνας του παραπονούμενου δεν προέκυψε τίποτε ύποπτο, η Υ.ΚΑ.Ν. δεν εδικαιολογείτο να φωτοτυπήσει το διαβατήριο του παραπονούμενου και να καταχωρήσει το φωτοαντίγραφό του στα αρχεία τους.

- Η ενέργεια της αυτή αποτελεί επεξεργασία προσωπικών δεδομένων περισσότερων από όσα είναι απαραίτητα για την εκπλήρωση του σκοπού της επεξεργασίας, που είναι η συλλογή και καταχώρηση πληροφοριών που αναφέρονται σε πρόσωπα που είναι ύποπτα για την εισαγωγή, διακίνηση και χρήση ναρκωτικών.

- Σε καμία δε περίπτωση δεν είχε η Υ.ΚΑ.Ν. εξουσία να συλλέξει και καταγράψει πληροφορίες που αφορούσαν τους γονείς του παραπονούμενου, δεδομένου ότι η έρευνα είχε διεξαχθεί γιατί ο παραπονούμενος είχε κριθεί ύποπτος για μεταφορά ναρκωτικών.

  Και στις δύο περιπτώσεις, η Υ.ΚΑ.Ν. συνέλεξε και επεξεργάστηκε στοιχεία που ήταν υπερβολικά/μη συναφή με τον σκοπό της επεξεργασίας που αναφέρθηκε πιο πάνω, κατά παράβαση του άρθρου 4(1)(γ) του Νόμου.

Γι' αυτό κρίνω ότι:

(α) Η Αστυνομία/ Υ.ΚΑ.Ν. δεν έπρεπε να συλλέξει και επεξεργασθεί προσωπικά δεδομένα του παραπονούμενου γιατί από τις διεξαχθείσες έρευνες δεν προέκυψε ότι αυτός ενέχεται σε παράνομες πράξεις που αφορούν τη διακίνηση, εμπορία και χρήση ναρκωτικών.

  Η δε φωτοτύπηση του διαβατηρίου του παραπονούμενου και καταχώρηση του φωτοαντίγραφου σε αρχείο της Αστυνομίας/ Υ.ΚΑ.Ν. παραβιάζει το άρθρο 4(1)(γ) του Νόμου.

(β) Η συλλογή και καταχώρηση/επεξεργασία προσωπικών δεδομένων των γονιών του έγινε κατά παράβαση του άρθρου 4(1)(γ) γιατί τα δεδομένα αυτά δεν ήταν συναφή με τον σκοπό της επεξεργασίας, δεδομένου ότι οι οποιεσδήποτε υπόνοιες αναφορικά με τον παραπονούμενο, οι οποίες εν πάση περιπτώσει δεν επαληθεύθηκαν, δεν τους αφορούσαν και οι προσωπικές πληροφορίες που δόθηκαν γι' αυτούς δεν ήταν ούτε απαραίτητες ούτε συναφείς σε σχέση με τον σκοπό για τον οποίο είχαν συλλεγεί.

Με βάση τα πιο πάνω η Αστυνομία/Υ.ΚΑ.Ν. πρέπει:

- Να μεριμνήσει ώστε να καταστραφούν όσα προσωπικά δεδομένα έχουν συλλεγεί υπό τις συνθήκες που αναφέρονται στις παρ. (α) και (β) και να με πληροφορήσει μέσα σε τρεις εβδομάδες από τη λήψη της παρούσας Απόφασης για τα μέτρα που έλαβε για υλοποίηση των πιο πάνω.

- Η Αστυνομία/Υ.ΚΑ.Ν. να δώσει τις κατάλληλες οδηγίες στα μέλη της για υλοποίηση της απόφασης και συμμόρφωση με το περιεχόμενό της.

Γούλλα Φράγκου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα.

| | |
|---|---|
| **Case title** | Complaint of the Consumers' Association in relation to the dispatch of marketing messages to mobile phones |
| **Decision date** | 26.02.2004 |
| **Reference details** (reference number; type and title of court/body; in original language and English [official translation, if available]) | Επίτροπος Προστασίας Προσωπικών Δεδομένων<br>Commissioner for the Protection of Personal Data |
| **Key facts of the case** (max. 500 chars) | The Consumers' Association complained to the Data Protection Commissioner about unsolicited SMS sent to mobile phones from a certain company (hereinafter 'company X') advertising sales in swimwear. From the Commissioner's investigation it emerged that the said company was in cooperation with another company (hereinafter 'company Y') from whom it obtained consumers' personal data and which had reassured company X that the use of the consumers' data was lawful as they had given their consent. The data was compiled by a third company (hereinafter 'Company Z') which belonged to the same group of companies as company Y The Commissioner's investigation revealed that the consent of the subjects of the data was not obtained, as it was required by section 15 of Law 138(I)/2001.[64] Also, the various officials of company Z supplied the Commission with conflicting versions of events and demonstrated an effort to misinform and deceive the Commissioner. |

[64] Cyprus/ The Processing of Personal Data (Protection of Individuals) Law N. 138(I)/2001.

| | |
|---|---|
| **Main reasoning/argumentation** (max. 500 chars) | The Commissioner found that company Z used to dispatch marketing messages without the consent of the receivers, in violation of section 15 of the law which provides that personal data cannot be processed by anyone for the purposes of direct marketing or provision of services, unless the data subject notifies his consent to the Commissioner in writing. Company Y was also found guilty of collecting and processing personal data in violation of section 4(1)(a) of the law which requires that the controller ensures that personal data are processed fairly and lawfully. |
| **Key issues (concepts, interpretations) clarified by the case** (max. 500 chars) | The Commissioner's office investigated in great detail the unclear situation which emerged as a result of the conflicting statements made by the various company officials, which included an on-site visit and personal interviews with the persons concerned, recorded this procedure in the decision and took this fact into consideration whilst imposing her fine. Also, the assurance of company X that they believed the subjects' consent had been obtained was sufficient in order to absolve company X from liability in this case. |
| **Results (sanctions) and key consequences or implications of the case** (max. 500 chars) | The Commissioner imposed a fine of 500 Cyprus Pounds (854 Euros) on Company Y and 1,000 Cyprus Pounds (1708 Euros) on company Z. In imposing these sanctions, the Commissioner took into consideration the fact that companies Y and Z did not demonstrate a willingness to co-operate with her office and offered contradictory information, but also the fact that they had since 2003 stopped sending unsolicited marketing messages and had destroyed their relevant database. |
| **Proposal of key words for data base** | Marketing SMS, unsolicited mail |

## Καταγγελία του Συνδέσμου Καταναλωτών σχετικά με την αποστολή Διαφημιστικών μηνυμάτων σε κινητά τηλέφωνα

1. Στις 25 Ιουνίου 2003, ο Κυπριακός Σύνδεσμος Καταναλωτών, ο οποίος ήταν δέκτης αρκετών καταγγελιών, υπέβαλε στο Γραφείο μου γραπτή καταγγελία σχετικά με τη λήψη διαφημιστικών μηνυμάτων SMS από καταναλωτές σχετικά με επικείμενες εκπτώσεις σε μαγιό της εταιρείας Χ.

Οι παραπονούμενοι καταναλωτές είχαν δηλώσει στο Σύνδεσμο ότι δεν είχαν καταχωρημένο στον τηλεφωνικό κατάλογο τον αριθμό του κινητού τηλεφώνου τους και ούτε είχαν συγκατατεθεί στη λήψη διαφημιστικών μηνυμάτων.

Περαιτέρω ο Σύνδεσμος ανέφερε ότι από πληροφορίες που έλαβε παραπονούμενος από την εταιρεία Χ, η εταιρεία αυτή φερόταν να είχε συνεργασία με την εταιρεία Α.Β. από την οποία έπαιρνε τα προσωπικά δεδομένα των καταναλωτών.

2. Έκτοτε το Γραφείο μου άρχισε σχετική, με την πιο πάνω καταγγελία, έρευνα για διαπίστωση τυχόν παράβασης της νομοθεσίας.

3. Για τον σκοπό αυτό απευθύναμε την 1η Ιουλίου 2003 επιστολή στην εταιρεία Woolworth και στην εταιρεία Α.Β. (που στο εξής θα αναφέρεται ως η Εταιρεία) ζητώντας συγκεκριμένες πληροφορίες σχετικά με τους ισχυρισμούς που αναφέρονταν στην καταγγελία.

4. Η εταιρεία Χ με επιστολή της με ημερομηνία 7 Αυγούστου 2003 μας ενημέρωσε ότι «έχουμε διαβεβαιώσεις από την Εταιρεία ότι η αποστολή τέτοιων μηνυμάτων στους συγκεκριμένους κατόχους κινητών τηλεφώνων, κατάσταση των οποίων μας έχουν προμηθεύσει, είναι καθόλα νόμιμη καθότι υπήρχε η συγκατάθεση των συνδρομητών».
Σε μεταγενέστερη επιστολή της με ημερομηνία 20 Αυγούστου 2003, η εταιρεία Χ ανάφερε, μεταξύ άλλων, ότι δεν διατηρούσε «άλλη» λίστα με ονόματα και κινητά τηλέφωνα, αφού η λίστα η οποία χρησιμοποιήθηκε ήταν και είναι στην κατοχή της Εταιρείας.

5. Στην επιστολή μας της 1ης Ιουλίου 2003 ζητήσαμε από την εταιρεία Α.Β. να μας πληροφορήσει κατά πόσο διαθέτει σε τρίτους καταλόγους με ονόματα, διευθύνσεις και άλλες πληροφορίες γιατί σε Γνωστοποίηση που η εταιρεία είχε υποβάλει στο Γραφείο μου αναφορικά με την τήρηση αρχείου με προσωπικά δεδομένα για σκοπούς μάρκετινγκ, είχε προσδιορίσει ως αποδέκτες των δεδομένων μόνο τη διεύθυνση της εταιρείας.
Σε απαντητική επιστολή της ημερομηνίας 10 Ιουλίου 2003, η Εταιρεία μας πληροφόρησε ότι οι πληροφορίες συλλέγονται από τους πελάτες της και δε δίνονται σε τρίτους. Σε μεταγενέστερη επιστολή της, η Εταιρεία αναφέρει, μεταξύ άλλων, ότι «ο όμιλος των εταιρειών μας συλλέγει τα προσωπικά δεδομένα των πελατών της κάθε εταιρείας».

6. Επειδή από την σχετική αλληλογραφία που είχε διεξαχθεί στα πλαίσια εξέτασης της καταγγελίας δεν κατορθώσαμε να πάρουμε τις απαραίτητες πληροφορίες και διευκρινήσεις, κρίθηκε σκόπιμη μια επίσκεψη στα γραφεία της Εταιρείας με σκοπό τη διεξαγωγή ελέγχου στα αρχεία της για διαπίστωση των συνθηκών κάτω από τις οποίες εκτελείται η επεξεργασία προσωπικών δεδομένων, ιδιαίτερα για σκοπούς "marketing".

7. Η επίσκεψη έγινε στις 20 Ιανουαρίου 2004 και κατά τη διάρκειά της είχαν υποβληθεί στους εκπροσώπους της Εταιρείας που παρεβρίσκοντο οι ακόλουθες ερωτήσεις:

(α) Εκτός από τα αρχεία των ασφαλιζόμενων και των γνωριμιών τα οποία είχε γνωστοποιήσει στο Γραφείο μας, αν διατηρούσαν και άλλα αρχεία με προσωπικά δεδομένα.
(β) Αν είχαν αποστείλει διαφημιστικό υλικό χωρίς τη συγκατάθεση των γνωριμιών.
(γ) Αν είχαν χρησιμοποιήσει το αρχείο γνωριμιών για σκοπούς προώθησης προϊόντων ή υπηρεσιών εταιρειών που δεν είναι μέλη του ομίλου τους.

Οι απαντήσεις στις πιο πάνω ερωτήσεις ήταν οι ακόλουθες:

(α) Ναι το αρχείο της A.B. E-Media Ltd
(β) Ναι
(γ) Όχι

Μας ελέχθη επίσης ότι χρησιμοποιούν το αρχείο A.B. E-Media ltd για σκοπούς που εξυπηρετούν συμφέροντα τρίτων – πελατών τους και ανέλαβαν να μας προμηθεύσουν με κατάλογο αυτών των πελατών τους.
Ανέφεραν επίσης ότι χρησιμοποιούν το αρχείο των πελατών τους για σκοπούς προώθησης προϊόντων και υπηρεσιών τους.

8. Σχετικά με την εταιρεία A.B. E-Media Ltd, η οποία ανήκει στον Όμιλο Εταιρειών A.B. Ltd αναφέρθη ότι είναι αυτή που διατηρεί αρχείο με αριθμούς κινητών τηλεφώνων και ότι τα μηνύματα στέλλονται από βάση δεδομένων που είναι στην Αμερική, δήλωση που αργότερα ανετράπη από τους ίδιους τους εκπροσώπους της Εταιρείας.
Στη συνέχεια μας δηλώθηκε ότι απαντήσεις στα ερωτήματά μας σχετικά με τις δραστηριότητες της A.B. E-Media Ltd μόνο ο διευθυντής της μπορούσε να μας δώσει αλλά απουσίαζε τη δεδομένη στιγμή.

9. Κατά τη διάρκεια της επίσκεψης αξιωματούχος/ διευθυντής της Εταιρείας είχε επανειλημμένα προβεί σε δηλώσεις που συγκρούονταν με δηλώσεις υπαλλήλων της Εταιρείας, καθώς και με δικές του προηγούμενες δηλώσεις.

10. Μετά την επίσκεψη στα Γραφεία της Εταιρείας ακολούθησε αλληλογραφία σκοπός της οποίας ήταν η διευκρίνηση ορισμένων θεμάτων που είχαν προκύψει κατά την επίσκεψη.

11. Στις 28 Φεβρουαρίου 2004 πήραμε επιστολή από το δικηγορικό γραφείο ΧΧ με την οποία μας πληροφόρησαν ότι ενεργούσαν εκ μέρους της Εταιρείας και ότι θα απαντούσαν στα ερωτήματα που είχαμε θέσει σαν αποτέλεσμα της επίσκεψης.
Στην επιστολή αυτή και σχετικά με την αποστολή διαφημιστικών μηνυμάτων, αναφέρεται ότι η Α.Β. E-Media Ltd διατηρεί αρχείο με προσωπικά δεδομένα τα οποία της δίνουν οι πελάτες της το οποίο χρησιμοποιεί για να αποστέλλει στη συνέχεια διαφημιστικά μηνύματα.
Παρατέθηκε κατάλογος των εταιρειών εκ μέρους των οποίων η Α.Β. E-Media Ltd αποστέλλει διαφημιστικά μηνύματα και αναφέρθηκε επίσης ότι η ίδια η Εταιρεία αποστέλλει διαφημιστικά μηνύματα σε πελάτες της ή συνεργάτες τους.
Σε απάντηση σχετικής επιστολής μας προς τις εταιρείες αυτές, ορισμένες από αυτές αρνήθηκαν ότι είχαν δώσει στην εταιρεία Α.Β. E-Media Ltd βάση δεδομένων με στοιχεία επικοινωνίας των πελατών τους.

12. Ακολούθησε συνάντηση στο Γραφείο μας στις 15 Σεπτεμβρίου 2004 στην οποία ήταν παρόντες ο νομικός σύμβουλος της Εταιρείας, ο διευθυντής της Α.Β. E-Media Ltd και ο κ. Ζ.

Ο διευθυντής της Α.Β. E-Media Ltd ανάφερε ότι η εταιρεία σταμάτησε την αποστολή διαφημιστικών μηνυμάτων SMS τον Σεπτέμβριο του 2003. Δήλωσε ότι την αρχική βάση δεδομένων για την αποστολή τέτοιων μηνυμάτων την είχαν πάρει από hackers που είχαν καταφέρει να εισβάλουν στα αρχεία της ΑΤΗΚ.

Ανάφερε επίσης ότι εσφαλμένα το Intercollege είχε περιληφθεί στον κατάλογο των εταιρειών εκ μέρους των οποίων έστελλαν διαφημιστικά μηνύματα και ότι, όσον αφορούσε την εταιρεία Χατζηκυριάκος & Υιοί, δεν τους είχε δώσει κατάλογο των πελατών της αλλά χρησιμοποιούσε τη βάση της Α.Β. E-Media Ltd για την αποστολή διαφημιστικών μηνυμάτων εκ μέρους της.

13. Σε μεταγενέστερη επιστολή του δικηγόρου της Εταιρείας ημερομηνίας 22 Σεπτεμβρίου 2004 αναφέρθηκε ότι η Α.Β. E-Media Ltd απέστελλε διαφημιστικά μηνύματα εκ μέρους πελατών της χρησιμοποιώντας τη δική της βάση δεδομένων.

14. Στην τελευταία επιστολή του νομικού συμβούλου της Εταιρείας της 1ης Φεβρουαρίου 2005 δίνεται άλλη εκδοχή ως την προέλευση και κατοχή της βάσης δεδομένων η οποία εχρησιμοποιείτο για την αποστολή διαφημιστικών μηνυμάτων.

15. Ανεξάρτητα από τα πιο πάνω, ήταν παραδεκτό ότι σε καμία περίπτωση δεν ελαμβάνετο η συγκατάθεση των παραληπτών των μηνυμάτων, όπως προβλέπεται στο άρθρο 15 του Νόμου 138(I)/2001 (που στη συνέχεια θα αναφέρεται ως «ο Νόμος») .

Από τα πιο πάνω, έχω ικανοποιηθεί ότι:

- Η Εταιρεία και η εταιρεία που ανήκει σε αυτή, η A.B. E-Media Ltd προέβαιναν στην αποστολή μηνυμάτων διαφημιστικού περιεχομένου χωρίς τη συγκατάθεση των παραληπτών των μηνυμάτων κατά παράβαση του άρθρου 15 του Νόμου.

- Συνέλεγαν και προέβαιναν στην επεξεργασία προσωπικών δεδομένων κατά παράβαση του άρθρου 4(1)(α) και (β) του Νόμου.

- Παρέλειψαν να γνωστοποιήσει στο Γραφείο μου όλα τα αρχεία που περιείχαν προσωπικά δεδομένα και/ή όλες τις επεξεργασίες προσωπικών δεδομένων που εκτελούσαν.

Το άρθρο 25 του Νόμου προβλέπει τις κυρώσεις που μπορεί να επιβάλει ο Επίτροπος για παράβαση των υποχρεώσεων των υπεύθυνων επεξεργασίας που πηγάζουν από το Νόμο, μεταξύ των οποίων είναι και η εξουσία για την επιβολή χρηματικής ποινής μέχρι £5000.

Κατά την επιμέτρηση της αρμόζουσας για την περίπτωση κυρώσεως έλαβα υπόψη μου όλα τα περιστατικά της υπόθεσης όπως αυτά εκτίθενται στη σχετική αλληλογραφία, την επίσκεψη λειτουργών του Γραφείου μου στα Γραφεία της Εταιρείας, καθώς και την επίσκεψη του νομικού συμβούλου και εκπροσώπων της Εταιρείας στο Γραφείο μου.

Ειδικότερα έλαβα υπόψη μου ότι (α) καθόλη τη διάρκεια της διαδικασίας εξέτασης της καταγγελίας/παραπόνου είχαν δοθεί τουλάχιστο τέσσερις διαφορετικές εκδοχές αναφορικά με το θέμα του τρόπου απόκτησης της βάσης των δεδομένων η οποία εχρησιμοποιείτο για την αποστολή διαφημιστικών μηνυμάτων, (β) οι διευθυντές και άλλοι εκπρόσωποι της Εταιρείας και της A.B. E-Media Ltd έδιναν αλληλοσυγκρουόμενες απαντήσεις, (γ) δεν είχε επιδειχθεί διάθεση συνεργασίας με τους λειτουργούς του Γραφείου μου και γενικά η όλη συμπεριφορά των αρμοδίων στελεχών της εταιρείας κατεδείκνυε μια προσπάθεια παραπλάνησης και εσφαλμένης πληροφόρησής μας.

Από την άλλη πλευρά δεν παρέλειψα να λάβω υπόψη και να αποδεχθώ ως αληθή τη δήλωση των διευθυντών της Εταιρείας και της A.B. E-Media Ltd ότι δεν αποστέλλουν πλέον διαφημιστικά μηνύματα χωρίς τη συγκατάθεση των παραληπτών, ότι έχουν καταστρέψει τη βάση δεδομένων την οποία είχαν χρησιμοποιήσει για την αποστολή διαφημιστικών μηνυμάτων και ότι οι μελλοντικές τους ενέργειες τόσον όσον αφορά το θέμα της αποστολής διαφημιστικών μηνυμάτων όσο και γενικά τις οποιεσδήποτε άλλες υποχρεώσεις τους που απορρέουν από το Νόμο θα είναι σύμφωνες με τις οικείες διατάξεις του Νόμου.

Παρά ταύτα θεωρώ ότι υπό τις περιστάσεις είναι επιτακτική η επιβολή χρηματικής ποινής για τις προαναφερθείσες παραβάσεις της νομοθεσίας.

Γι' αυτό επιβάλλω στην A.B. Ltd χρηματική ποινή £500 και την A.B. E-Media Ltd χρηματική ποινή £1000.

Γούλλα Φράγκου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα

| | |
|---|---|
| **Case title** | List with Subscribers' Codes on the Internet |
| **Decision date** | 21.11.2005 |
| **Reference details** (reference number; type and title of court/body; in original language and English [official translation, if available]) | Επίτροπος Προστασίας Προσωπικών Δεδομένων<br>Commissioner for the Protection of Personal Data |
| **Key facts of the case** (max. 500 chars) | The Commissioner was informed that a webpage was located on the internet containing the list of access codes for one of the services provided by the semi-governmental Cyprus Telecommunication Authority (CYTA) known as "i-choice". As a result, the Commissioner asked CYTA to inform her office as to the measures taken to remedy the problem and to avoid similar occurrences in the future. CYTA responded that after investigation it established that the codes published on the said webpage were in use by subscribers two and a half years ago but, given the fact that |

| | |
|---|---|
| | it could not specify who the codes belonged it, it did not inform all its customers so as not to cause panic. Following the 2005 publication of codes on the internet, CYTA sent a letter to its affected customers urging them to change their codes, but since not all of them responded, it planned to send additional letters to them. CYTA also mentioned that a complaint had been filed with the police regarding this case |
| **Main reasoning/argumentation** (max. 500 chars) | The Commissioner stated that CYTA and all other companies handling personal data must take all necessary measures to ensure that access to their systems by hackers is impossible; must be in a position to locate immediately instances of unauthorised access and must inform all subscribers affected to enable them to take measures to protect their personal data even if this is likely to cause panic. The Commissioner notes that, on the other hand, due to continuous technological development, all internet users must bear in mind that no internet system is absolutely safe as new weaknesses are discovered daily. CYTA assured the Commissioner that according to audits conducted by external organisations, it offers a high standard of protection and intends to take additional measures. |
| **Key issues (concepts, interpretations) clarified by the case** (max. 500 chars) | The Commissioner found that, given that CYTA has taken some measures to address the problem and in view of the fact that internet systems can never be 100% safe, no sanctions were imposed. |
| **Results (sanctions) and key consequences or implications of the case** (max. 500 chars) | No fine or other penalty was imposed. The admission of CYTA that for the 2005 internet publication of access codes no subscribers were informed in order to avoid panic was not taken into account in the decision not to impose a fine. |
| **Proposal of key words for data base** | Internet system, hackers, access codes |

## **Κατάλογος με κωδικούς συνδρομητών στο Διαδίκτυο**

ΑΠΟΦΑΣΗ

1.1 Τον Φεβρουάριο του 2005 εντοπίστηκε σελίδα στο Διαδίκτυο η οποία περιείχε κατάλογο με κωδικούς πρόσβασης της ευρυζωνικής υπηρεσίας της Cytanet i-choice.

Σχετικά με το περιστατικό αυτό, για το οποίο είχε υποβληθεί και παράπονο στο Γραφείο μας, ζητήσαμε από την Α.ΤΗ.Κ. να μας αναφέρει πότε ανακάλυψαν την «κλοπή» των κωδικών, σε τι ενέργειες είχαν προβεί για να ενημερώσουν τους συνδρομητές τους, τι μέτρα έχουν λάβει για αποφυγή επανάληψης τέτοιων περιστατικών και κατά πόσο έγιναν έρευνες είτε από την Α.ΤΗ.Κ είτε από την Αστυνομία και ποιο ήταν το αποτέλεσμα τους.

1.2 Η Α.ΤΗ.Κ μας ανάφερε ότι μετά από λεπτομερή έλεγχο που έγινε στον εν λόγω κατάλογο, διαφάνηκε ότι οι κωδικοί αυτοί ήταν κωδικοί πρόσβασης οι οποίοι χρησιμοποιούνταν από πελάτες πριν από δυόμισι χρόνια. Κατά την περίοδο εκείνη κάποιοι κατάφεραν να διεισδύσουν στο δίκτυο i-choice και να έχουν πρόσβαση σε κάποιους κωδικούς. Δεν είχε γίνει τότε οποιαδήποτε δημοσίευση καταλόγου με τους κωδικούς. Ανάφερε επίσης ότι οι πελάτες στους οποίους ανήκαν οι κωδικοί δεν μπορούσαν να συγκεκριμενοποιηθούν και έτσι δεν ενημερώθηκαν τότε όλοι οι πελάτες για να αποφευχθεί πανικός.

1.3 Μετά τη δημοσίευση καταλόγου με τους κωδικούς στο Διαδίκτυο τον Φεβρουάριο του 2005, η Α.ΤΗ.Κ. επικοινώνησε με τους επηρεαζόμενους πελάτες με ταχυδρομείο και τους προέτρεψε να αλλάξουν τους κωδικούς τους. Σε όσους δεν είχα ανταποκριθεί σ' αυτήν την επικοινωνία, η Α.ΤΗ.Κ. σκόπευε να στείλει νέα υπενθύμιση μέσω ηλεκτρονικού ταχυδρομείου και συστημένης επιστολής.

Η Α.ΤΗ.Κ. στην απάντησή της αναφέρθηκε λεπτομερώς στα μέτρα που είχε λάβει/ προτίθεται να λάβει για την ασφάλεια και προστασία των συστημάτων του Οργανισμού και των προσωπικών δεδομένων των πελατών της

1.4 Αναφέρθηκε επίσης στην εν λόγω επιστολή ότι η υπόθεση έχει καταγγελθεί και διερευνάται από την Αστυνομία

2 Η Α.ΤΗ.Κ. καθώς και όλες οι εταιρείες / αρχές / οργανισμοί που χειρίζονται προσωπικά δεδομένα θα πρέπει να λαμβάνουν όλα τα απαραίτητα μέτρα ώστε να μην είναι εφικτή από μη εξουσιοδοτημένα πρόσωπα / hackers (crackers) η πρόσβαση στα συστήματα τους και στα προσωπικά δεδομένα των πελατών τους.

Επίσης πρέπει να είναι σε θέση να εντοπίζουν άμεσα περιστατικά τέτοιας μη εξουσιοδοτημένης πρόσβασης. Τα περιστατικά αυτά δεν θα πρέπει να αποσιωπούνται αλλά να ανακοινώνονται αμέσως μετά τον εντοπισμό τους με συμβουλές ως προς την αντιμετώπιση τους, ώστε οι επηρεαζόμενοι πελάτες να προβούν σε όλες τις απαραίτητες ενέργειες για προστασία των προσωπικών τους δεδομένων, έστω και αν τέτοια ανακοίνωση πιθανό να δημιουργήσει πανικό και να επηρεάσει την φήμη και την αξιοπιστία τους.

3 Από την άλλη πλευρά, λόγω της συνεχούς εξέλιξης της τεχνολογίας, όλοι οι χρήστες του Διαδικτύου πρέπει να έχουν υπόψη τους ότι κανένα σύστημα στο Διαδίκτυο δεν είναι απόλυτα ασφαλισμένο λόγω του ότι καθημερινά ανακαλύπτονται νέες αδυναμίες στα λειτουργικά συστήματα των υπολογιστών και στα προγράμματα επικοινωνίας που χρησιμοποιούνται στο Διαδίκτυο, οι οποίες μπορούν να χρησιμοποιηθούν για απόκτηση μη εξουσιοδοτημένης πρόσβασης σε τέτοια συστήματα.

4 Η Α.ΤΗ.Κ. διαβεβαιώνει ότι σύμφωνα με ελέγχους από εξωτερικούς οίκους διαθέτει σήμερα υψηλό επίπεδο προστασίας, το οποίο συνεχίζει να ενημερώνει με ελέγχους ασφαλείας και προτίθεται να λάβει επιπρόσθετα μέτρα.

Με βάση τα πιο πάνω κατάληξα ότι υπό τις περιστάσεις, δεν θεωρώ ότι θα πρέπει να επιβληθεί οποιαδήποτε χρηματική ή άλλη ποινή στην Α.ΤΗ.Κ για την υπόθεση αυτή.

Τυχόν επανάληψη όμως παρόμοιου περιστατικού στο μέλλον δεν θα έχει βεβαίως την ίδια αντιμετώπιση.

Γούλλα Φράγκου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα.

| | |
|---|---|
| **Case title** | Self-initiated investigation for the breach of the obligation to safely store patients' personal data at the old General Hospital of Nicosia |
| **Decision date** | 07.12.2007 |

| | |
|---|---|
| **Reference details** (reference number; type and title of court/body; in original language and English [official translation, if available]) | Επίτροπος Προστασίας Προσωπικών Δεδομένων<br>Commissioner for the Protection of Personal Data |
| **Key facts of the case** (max. 500 chars) | Following an article in the press suggesting that patients' files at the old hospital had abandoned in the old building and were available for everyone to see, the Commissioner used its powers under the law to conduct a self-initiated investigation in order to ascertain whether any measures had been taken for the protection of patients' personal data, in accordance with section 10 of Law 138(I)/2001[65] law which requires the controller to "take the appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing." For this purpose, two officers from the Commissioner's offices visited the old hospital building who found that access to the wing in question was free and unobstructed and that patients' files were indeed left open and exposed on desks, open shelves and even on the floor in some cases. A subsequent visit revealed that some measures had meanwhile been taken to improve this situation and that the personal files of patients had been removed in order to be destroyed. The Permanent Secretary of the Ministry of Health argued that a team from the Department of Public Works was responsible for the exposure of the files, since it started works on the old building without informing the Ministry of Health in advance of the precise date. Also, the Ministry argued that the guards of a private security company which had been hired to guard the building did not follow instructions and were thus replaced. |
| **Main reasoning/argumentation** (max. 500 chars) | The Commissioner found that personal data contained in medical examinations and tests constitute sensitive data which must be afforded increased protection given that their processing, which includes preservation, notification, availability etc is prohibited as a rule and allowed only exceptionally in the cases set out in section 6(2) of Law 138(I)2001.[66] The Commissioner also invoked section 10(1) of the law which provides that the processing of data |

[65] Cyprus/ The Processing of Personal Data (Protection of Individuals) Law N. 138(I)/2001.

[66] Section 6(2) reads: (2) Notwithstanding the provisions of subsection (1), the collection and processing of sensitive data, is permitted, when one or more of the following conditions are fulfilled: (a) the data subject has given his explicit consent, unless such consent has been obtained illegally or is contrary to accepted moral values or a specific law provides that consent does not lift the prohibition; (b) processing is necessary so that the controller may fulfil his obligations or carry out his duties in the field of employment law; (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; (d) processing is carried out by a foundation, association or other non-profit-making organisation which has political, philosophical, religious or trade-union aims, and relates solely to its members and such other persons with whom the said association, foundation or organisation retains relations by reason of its purposes. Such data may be communicated to third parties only if the data subject gives his consent; (e) the processing relates solely to data which are made public by the data subject or are necessary for the establishment, exercise or defence of legal claims before the Court, (f) the

| | |
|---|---|
| | is confidential and may be carried out only by persons acting under the authority of the controller or the processor and only upon instructions from the controller, as well as section 10(3) which requires the controller to take the appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing. The Commissioner referred to the minutes of two meetings conducted for the spatial management of the old hospital building, according to which no decision was made for the management of the documents containing sensitive data of patients and stated that it was also proved in practice that no measures were taken for their protection and the Ministry of Health did not monitor the implementation of decisions concerning the protection of the building. As a result, the Commissioner found there was a violation of sections 10(3) and 10(4)[67] of the law |
| **Key issues (concepts, interpretations) clarified by the case** (max. 500 chars) | |
| **Results (sanctions) and key consequences or implications of the case** (max. 500 chars) | The Commissioner imposed a fine of 1,500 Cyprus Pounds (2,563 Euros), taking into consideration the willingness of the Permanent Secretary of the Ministry of Health to immediately adopt measures for the safe keeping or destruction of the personal data located in the old hospital building. |
| **Proposal of key words for data base** | Sensitive data, patients' files, hospital protection measures |

processing relates to medical data and is performed by a person providing health services by profession and has a duty of confidentiality or is subject to relevant codes of conduct, on condition that the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or the management of health-care services; g) processing is necessary for the purposes of national needs or national security, as well as criminal and reform policy, and is performed by a service of the Republic or an Organisation or Foundation authorized for this purpose by a service of the Republic and relates to the detection of crimes, criminal convictions, security measures and investigation of mass destructions; (h) processing is performed solely for statistical, research, scientific and historical purposes, on condition that all the necessary measures are taken for the protection of the data subjects; (i) processing is performed solely for journalistic purposes or in the framework of artistic expression and as long as the right to privacy and family life is not violated.

[67] Section 10(4) reads: If processing is performed by the processor, the assignment for the processing must be made in writing. The assignment must provide that the processor shall perform the processing only upon instructions from the controller and that the remaining obligations set out in this section shall also lie on the processor.

**Αυτεπάγγελτη έρευνα για παράβαση της υποχρέωσης για την ασφαλή φύλαξη των προσωπικών δεδομένων των ασθενών στο παλαιό Γενικό Νοσοκομείο Λευκωσίας**

**Α Π Ο Φ Α Σ Η**

Σύμφωνα με δημοσίευμα της εφημερίδας «Ο Φιλελεύθερος» στην έκδοσή της ημερομ. 19/3/2007, με τίτλο «Όπου σ' έβρω τζι' όπου με έβρεις», το παλιό Νοσοκομείο Λευκωσίας εγκαταλείφθηκε στο έλεος του χρόνου, αλλά και όλων όσων μπαινόβγαιναν ανενόχλητοι σ' αυτό και υπήρχαν πεταμένοι απροστάτευτοι φάκελοι και ακτινογραφίες με προσωπικά δεδομένα ασθενών που αφορούσαν ιατρικές εξετάσεις.

2. Με βάση το δημοσίευμα αυτό και ασκώντας τις εξουσίες που μου χορηγεί το άρθρο 23(η) του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου του 2001, αποφάσισα να διενεργήσω αυτεπάγγελτη έρευνα με σκοπό να διαπιστώσω κατά πόσο τα μέτρα για την ασφάλεια και την προστασία των προσωπικών δεδομένων που διατηρούνταν στο παλαιό Νοσοκομείο Λευκωσίας ήταν ικανοποιητικά και σύμφωνα με τις σχετικές διατάξεις του άρθρου 10 του Νόμου 138(Ι)/2001.

3. Για το σκοπό αυτό, δύο ειδικά εξουσιοδοτημένοι από εμένα λειτουργοί του Γραφείου μου επισκέφθηκαν την ίδια ημέρα το παλαιό Νοσοκομείο Λευκωσίας και συγκεκριμένα τη Ψυχιατρική Πτέρυγα, όπου διαπίστωσαν ότι διεξάγονταν εργασίες επιδιόρθωσης/ επισκευής από υπαλλήλους του Τμήματος Δημοσίων Έργων.

4. Οι λειτουργοί του Γραφείου μου εισήλθαν από την κεντρική είσοδο του Νοσοκομείου χωρίς να τους ζητηθούν οποιεσδήποτε πληροφορίες από το φρουρό που βρισκόταν εκεί και προχώρησαν στο κτίριο της Ψυχιατρικής Κλινικής χωρίς να συναντήσουν οποιεσδήποτε σημάνσεις για απαγόρευση της εισόδου στο χώρο ή οποιαδήποτε φυσικά εμπόδια. Στην είσοδο της Ψυχιατρικής Κλινικής, η πόρτα της οποίας ήταν ανοικτή, συνάντησαν τη Γραμματειακή Λειτουργό του Νοσοκομείου, η οποία συμπτωματικά βρισκόταν στην πτέρυγα.

5. Οι λειτουργοί του Γραφείου μου εισήλθαν στο χώρο όπου διαπίστωσαν ότι υπήρχαν εγκαταλειμμένα και απροστάτευτα έγγραφα με προσωπικά δεδομένα ασθενών (που είχαν νοσηλευτεί στην πτέρυγα) όπως εγκεφαλογραφήματα, ιατρικές εκθέσεις (reports), φάκελοι, μητρώα ασθενών (βιβλία), ακτινογραφίες και ένα δελτίο ταυτότητας ασθενούς.

Τα πιο πάνω έγγραφα βρίσκονταν αφύλακτα και εκτεθειμένα σε ανοικτούς φοριαμούς, ανοικτά ράφια, γραφεία και στο πάτωμα, έτσι που ο οποιοσδήποτε τρίτος περιλαμβανομένων των υπαλλήλων του Τμήματος Δημοσίων Έργων θα μπορούσε να έχει εύκολη πρόσβαση σ' αυτά, να τα καταστρέψει ή και να τα υποκλέψει/ υπεξαιρέσει.

6. Με επιστολή μου προς το Γενικό Διευθυντή Υπουργείου Υγείας, με αρ. φακ. Α/Π 11.17.001 24/2007 και ημερομ. 21/3/2007, ζήτησα τις απόψεις/ θέσεις του σχετικά με τις πιο πάνω διαπιστώσεις και τον κάλεσα να λάβει αμέσως τα απαραίτητα μέτρα για την ασφάλεια και προστασία των εγγράφων/ εντύπων που περιείχαν προσωπικά δεδομένα και βρίσκονταν στο χώρο του παλαιού Νοσοκομείου.

7. Ο Γενικός Διευθυντής του Υπουργείου Υγείας, με επιστολή του με αρ. φακ. Υ.Υ.5.24.13(2) και ημερομ. 28/3/2007, δεν αμφισβήτησε τις διαπιστώσεις των Λειτουργών του Γραφείου μου ότι κατά τον έλεγχο που διενήργησαν στις 19/3/2007 βρέθηκαν αφημένα έγγραφα με προσωπικά δεδομένα ασθενών χωρίς να ληφθούν μέτρα ασφάλειας, αλλά με πληροφόρησε για ορισμένα μέτρα που λήφθηκαν εκ των υστέρων για την ασφάλεια των δεδομένων. Όταν στη συνέχεια λειτουργοί του Γραφείου επισκέφθηκαν ξανά για σκοπούς ελέγχου το παλαιό Νοσοκομείο Λευκωσίας στις 3/4/2007, διαπίστωσαν ότι λήφθηκαν κάποια μέτρα που βελτίωσαν την κατάσταση και ακολούθως στις 29/5/2007 διαπίστωσαν ότι το υλικό με τα δεδομένα προσωπικού χαρακτήρα είχε μεταφερθεί για καταστροφή με τη μέθοδο της ανακύκλωσης.

8. Σε συνάντηση μου με το Γενικό Διευθυντή του Υπουργείου Υγείας, που έγινε στο Γραφείο μου στις 3/5/2007, ο Γενικός Διευθυντής δεν αμφισβήτησε τις διαπιστώσεις των Λειτουργών του Γραφείου μου.

9. Ο Γενικός Διευθυντής Υπουργείου Υγείας, με τις επιστολές του με αρ. φακ. Υ.Υ.5.24.13(2) και με ημερομ. 14/5/2007 και 30/7/2007, ανέφερε ότι έγιναν συσκέψεις πριν τη μεταστέγαση του νοσοκομείου στο καινούργιο κτίριο και λήφθηκαν αποφάσεις για συγκεκριμένα μέτρα ασφάλειας. Στην επιστολή του ημερομ. 14/5/2007, ο Γενικός Διευθυντής Υπουργείου Υγείας ανέφερε, μεταξύ άλλων, ότι συνεργείο του Τμήματος Δημοσίων Έργων άνοιξε δωμάτια στην ψυχιατρική πτέρυγα και ξεκίνησε τις εργασίες χωρίς να ειδοποιήσει το Υπουργείο για την ακριβή ημερομηνία έναρξης των εργασιών, γι' αυτό βρέθηκαν αφύλακτα προσωπικά δεδομένα χωρίς να ληφθούν κατάλληλα μέτρα ασφάλειας και ότι οι φρουροί δεν εφάρμοσαν τις οδηγίες που τους είχαν δοθεί και γι' αυτό η εταιρεία ασφάλειας αντικατέστησε όλα τα πρόσωπα που απασχολούσε για τη φύλαξη του χώρου του παλαιού Γενικού Νοσοκομείου Λευκωσίας. Στην επιστολή του με ημερομηνία 30/7/2007, ο Γενικός Διευθυντής

επανέλαβε τον ισχυρισμό ότι τα μέτρα ασφάλειας παραβιάστηκαν λόγω της εμπλοκής του Τμήματος Δημοσίων Έργων.

10. Σύμφωνα με τον περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμο του 2001 (Ν. 138(Ι)/2001 και 37(Ι)/2003):

(α) Τα προσωπικά δεδομένα που περιέχουν οι ιατρικές εξετάσεις/ αναλύσεις είναι ευαίσθητα δεδομένα, τα οποία πρέπει να τυγχάνουν αυξημένης προστασίας δεδομένου ότι η επεξεργασία τους (η οποία περιλαμβάνει τη φύλαξη, κοινοποίηση, διάθεση κλπ) κατά κανόνα απαγορεύεται, επιτρέπεται δε κατ' εξαίρεση μόνο στις περιπτώσεις που αναφέρονται στο εδάφιο (2) του άρθρου 6 του Νόμου.

(β) Σύμφωνα με τις διατάξεις του άρθρου 10(1) του Νόμου «η επεξεργασία δεδομένων είναι απόρρητη. Διεξάγεται αποκλειστικά και μόνο από πρόσωπα που τελούν υπό τον έλεγχο του υπεύθυνου επεξεργασίας ή του εκτελούντος την επεξεργασία και μόνο κατ' εντολή του».

(γ) Σύμφωνα δε, με τις διατάξεις του εδαφίου (3) του ίδιου άρθρου, «ο υπεύθυνος επεξεργασίας οφείλει να λαμβάνει τα κατάλληλα οργανωτικά και τεχνικά μέτρα για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας».

11. Όπως φαίνεται από το περιεχόμενο των Πρακτικών των συσκέψεων ημερομ. 5/9/2006 και 30/8/2006 που πραγματοποιήθηκαν για τη διαχείριση του χώρου και του κτιρίου του παλαιού Γενικού Νοσοκομείου Λευκωσίας, καμία απόφαση δεν είχε ληφθεί όσον αφορά τη διαχείριση εγγράφων που περιείχαν προσωπικά δεδομένα ασθενών τα οποία εβρίσκοντο στο Παλαιό Νοσοκομείο Λευκωσίας και τα μέτρα ασφάλειάς τους. Ακόμα και εάν γίνει δεκτό ότι υπήρχε σχεδιασμός και πρόγραμμα για την ασφάλεια των κτιρίων, όπως αποδείχθηκε στην πράξη δεν πάρθηκαν εύλογα μέτρα ασφάλειας, αφού το Υπουργείο Υγείας δεν άσκησε οποιοδήποτε έλεγχο σε όσους είχε αναθέσει την ευθύνη υλοποίησης συγκεκριμένων αποφάσεων που αφορούσαν την ασφάλεια των κτιρίων (παραδοχή ότι χωρίς συνεννόηση το Τμήμα Δημοσίων Έργων άφησε ξεκλείδωτους τους χώρους με τα αφύλακτα δεδομένα, παραδοχή ότι μεταγενέστερα συμπληρώθηκε η περίφραξη του χώρου του παλαιού κτιρίου του Γενικού Νοσοκομείου Λευκωσίας, παραδοχή ότι οι φρουροί της εταιρείας ασφάλειας μεταγενέστερα αντικαταστάθηκαν επειδή δεν φύλαξαν το χώρο).

12. Οι διαπιστώσεις των λειτουργών του Γραφείου μου ότι κατά τον έλεγχο που διενήργησαν στις 19/3/2007 στο χώρο της ψυχιατρικής κλινικής του παλαιού Νοσοκομείου Λευκωσίας είχαν αφεθεί ευαίσθητα προσωπικά δεδομένα ασθενών χωρίς να ληφθούν τα απαραίτητα για την περίπτωση μέτρα ασφαλείας, δεν αμφισβητήθηκαν. Οι διαπιστώσεις αυτές αναφέρονται και σχετίζονται με τη μεταστέγαση του παλαιού Γενικού Νοσοκομείου σε νέο κτίριο και συνίστανται στη μη ικανοποιητική εποπτεία της υλοποίησης των απαραίτητων μέτρων ασφάλειας για τη φύλαξη τόσο του χώρου όσο και του τυχόν περιεχομένου των κτιρίων, όπως εγγράφων που περιείχαν προσωπικά δεδομένα.

Όσον αφορά οποιαδήποτε έγγραφα ή έντυπα που περιείχαν προσωπικά δεδομένα τα οποία παρέμειναν στο παλαιό Γενικό Νοσοκομείο μετά τη μεταστέγασή του, ακόμα και αν δεχθούμε ότι αυτά δεν ήταν απαραίτητο να διατηρηθούν, θα έπρεπε να καταστραφούν για να μην υπάρχει η δυνατότητα να αποκαλυφθεί το περιεχόμενό τους.

Σε επιστολή του Γενικού Διευθυντή του Υπουργείου Υγείας με ημερομηνία 30 Ιουλίου 2007 και σε αντίγραφο επιστολής της Διευθύντριας των Ιατρικών Υπηρεσιών και Υπηρεσιών Δημόσιας Υγείας εκφέρονται ορισμένες απόψεις ως προς το ποιος ήταν υπεύθυνος για το συμβάν, θεωρώ όμως ότι έστω και αν είχαν προσληφθεί εμπειρογνώμονες για το σχεδιασμό και υλοποίηση της μεταστέγασης, την ευθύνη της γενικής εποπτείας και διακρίβωσης της συμμόρφωσης όλων των εμπλεκομένων είχε το Υπουργείο.

13. Έχοντας υπόψη όλα τα πιο πάνω κρίνω ότι στην υπό εξέταση υπόθεση υπήρξε παράβαση των διατάξεων του άρθρου 10(3) και (4) του Νόμου 138(I)/2001 που αναφέρονται στην παρ. 10 πιο πάνω και αφού έλαβα υπόψη όλα όσα αναφέρθηκαν από το Γενικό Διευθυντή του Υπουργείου καθώς και την προθυμία του να φροντίσει για την άμεση λήψη των απαραίτητων μέτρων που θα συνέτειναν στην εξασφάλιση ικανοποιητικής ασφάλειας ή για την καταστροφή των προσωπικών δεδομένων που ευρίσκονταν στο χώρο του παλαιού Γενικού Νοσοκομείου αποφάσισα ότι η υπό τις περιστάσεις ενδεικνυόμενη κύρωση είναι η επιβολή της χρηματικής ποινής των χιλίων πεντακοσίων λιρών (£1.500).

Γούλλα Φράγκου
Επίτροπος Προστασίας Δεδομένων Προσωπικού Χαρακτήρα

| | |
|---|---|
| **Case title** | Complaint no. A/P5/2008 against the Permanent Secretary of the Ministry of Health for failure to locate the medical file of a patient at the Nicosia General Hospital |
| **Decision date** | 24.07.2008 |
| **Reference details** (reference number; type and title of court/body; in original language and English [official translation, if available]) | Επίτροπος Προστασίας Προσωπικών Δεδομένων<br>Commissioner for the Protection of Personal Data |
| **Key facts of the case** (max. 500 chars) | The complainant had filed a complaint to the Ombudsman for the failure of the Nicosia General Hospital to locate his medical file. The Ministry of Health informed the Ombudsman that the complainant's file could not be located as a result of the transfer of the hospital to its new building. The Ombudsman referred the case to the Commissioner for the Protection of Personal Data for investigation. The Ministry of Health did not respond to the Commissioner's repeated letters, upon which the Commissioner concluded that the complainant's file had indeed been irretrievably lost. |
| **Main reasoning/argumentation** (max. 500 chars) | The Commissioner referred to section 17 of the Law on Protection of the Rights of Patients of 2004 (N. 1(I)/2005) according to which the competent health service provider is obliged to maintain medical records where the progress of the patient's treatment is recorded, including detailed information on the patient's identity, the treatment applied, previous medical history, the diagnosis, etc. Under section 18 of the same law, a patient has the rights of information, access and objection in relation to data concerning himself included in the medical record. The right to be informed, to have access to and to object to the processing of data relating to one's person are also safeguarded in sections 11, 12, 13 and 14 of the Law on the Protection of Personal Data N. 138(I)/2001. Furthermore, the Commissioner found there was a violation section 10(3) of Law on the Protection of Personal Data N. 138(I)/2001, which requires the controller to take the appropriate organizational and technical measures for the security of data and their protection against accidental or unlawful destruction, accidental loss, alteration, unauthorised dissemination or access and any other form of unlawful processing**,** as well as a violation of section 17 of the Law on Protection of the Rights of Patients of 2004 (N. 1(I)/2005) (above) liability for which does not require the existence of intent. |
| **Key issues (concepts, interpretations) clarified by the case** (max. 500 chars) | The Commissioner's decision establishes that the data controller has a strict liability to maintain data and offer access to such data to the data's subject, breach of which leads to an offence irrespective of whether there was intent on the part of the controller or not. |

| | |
|---|---|
| **Results (sanctions) and key consequences or implications of the case** (max. 500 chars) | A fine of Euros 2,000 was imposed on the Ministry of Health. |
| **Proposal of key words for data base** | Hospital, medical file, lost |

## Παράπονο με αρ. Α/Π 5/2008 κατά του Γενικού Διευθυντή Υπουργείου Υγείας για αδυναμία εντοπισμού ιατρικού φακέλου ασθενούς του Γενικού Νοσοκομείου Λευκωσίας

## Α Π Ο Φ Α Σ Η

Ο κ. Σ.Α. υπέβαλε στις 12 Ιανουαρίου 2007, παράπονο στο Γραφείο της Επιτρόπου Διοικήσεως κατά του Γενικού Νοσοκομείου Λευκωσίας. Ο παραπονούμενος ενεπλάκη σε οδικό δυστύχημα και νοσηλεύτηκε στο θάλαμο του Ορθοπεδικού Τμήματος του Γενικού Νοσοκομείου Λευκωσίας. Το Νοέμβριο του 2006 αποτάθηκε στη Διεύθυνση του Νοσοκομείου για να του δοθεί ο ιατρικός φάκελος του για σκοπούς αγωγής ενώπιον δικαστηρίου.

2. Ο Γενικός Διευθυντής του Υπουργείου Υγείας, με επιστολή που απέστειλε στην Επίτροπο Διοικήσεως στις 24 Μαΐου 2007, την πληροφόρησε ότι ο φάκελος του παραπονούμενου δεν κατέστη δυνατό να ανευρεθεί. Ο λόγος, όπως ανέφερε, οφείλετο στην επείγουσα μεταστέγαση του Γενικού Νοσοκομείου Λευκωσίας, η οποία δεν επέτρεψε την ταξινόμηση και αρχειοθέτηση όλων των φακέλων στις νέες εγκαταστάσεις.

3. Η Επίτροπος Διοικήσεως, με επιστολή της με αρ. φακ. 74/2007 και ημερομ. 5/6/2007, μου κοινοποίησε την Έκθεση της αναφορικά με το παράπονο του κ. Σαμίρ Αρναούτ με αρ. Α/Π 74/2007 και ημερομ. 5/6/2007 κατά του Υπουργείου Υγείας, ώστε να επιληφθώ λόγω αρμοδιότητας του θέματος της ασφαλούς φύλαξης και προστασίας των προσωπικών δεδομένων του παραπονούμενου.

4. Η Επίτροπος Διοικήσεως, με επιστολή της με αρ. φακ. Α/Π 74/2007 και ημερομ. 19/11/2007, ενημέρωσε τον παραπονούμενο ότι ο Γενικός Διευθυντής του Υπουργείου Υγείας την ενημέρωσε ξανά περί το Νοέμβριο του

2007, ότι ο ιατρικός του φάκελος δεν κατέστη δυνατό να ανευρεθεί (ο φάκελος του Υπουργείου Υγείας με αρ. Υ.Υ. 11.17.07.1.182 είναι σχετικός).

5.1 Σύμφωνα με το άρθρο 17 του περί Κατοχύρωσης και Προστασίας των Δικαιωμάτων των Ασθενών Νόμου του 2004 (Ν. 1(Ι)/2005), ο αρμόδιος παροχέας υπηρεσιών υγείας, οφείλει να τηρεί ιατρικά αρχεία, όπου εμφαίνεται η πορεία της θεραπείας του ασθενή. Τα αρχεία αυτά περιλαμβάνουν λεπτομερή στοιχεία τα οποία προσδιορίζουν την ταυτότητα του ασθενή και του αρμόδιου παροχέα υπηρεσιών υγείας, καθώς και ιατρική πληροφόρηση αναφορικά με τη θεραπεία που λαμβάνει ο ασθενής, το προηγούμενο ιατρικό ιστορικό του, τη διάγνωση της παρούσας ιατρικής κατάστασης του και της θεραπευτικής αγωγής που παρέχεται.

Ανάλογα με την περίπτωση, η διεύθυνση του ιατρικού ιδρύματος ή ο αρμόδιος παροχέας υπηρεσιών υγείας έχουν την ευθύνη για την τήρηση και φύλαξη τακτικών και ενημερωμένων ιατρικών αρχείων, σύμφωνα με τους περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμους του 2001 και 2003.

5.2 Βάσει του άρθρου 18 του Ν. 1(Ι)/2005, ο ασθενής έχει δικαίωμα ενημέρωσης, πρόσβασης και αντίρρησης σε σχέση με πληροφορίες που αφορούν τον ίδιο που περιλαμβάνονται στα ιατρικά αρχεία και κατά την άσκηση των δικαιωμάτων αυτών εφαρμόζονται αντίστοιχα, τηρουμένων των αναλογιών, οι διατάξεις των άρθρων 11 έως 14 των περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμων του 2001 και 2003 και των περί Επεξεργασίας Δεδομένων (Άδειες και Τέλη) Κανονισμών του 2002. Το δικαίωμα πρόσβασης του ασθενούς στα ιατρικά του αρχεία του παρέχει τη δυνατότητα να λαμβάνει, άμεσα ή έμμεσα δια του νομίμου αντιπροσώπου του, πληροφορίες που είναι καταχωρημένες στα αρχεία αυτά ή αντίγραφο ή απόσπασμα αυτών.

5.3 Σύμφωνα με τις πρόνοιες του άρθρου 25 του Ν. 1(Ι)/2005, παροχέας υπηρεσιών υγείας που παραβιάζει οποιαδήποτε από τις διατάξεις του άρθρου 17 είναι ένοχος αδικήματος και, τηρουμένων των αναλογιών, τυγχάνουν εφαρμογής οι διατάξεις των άρθρων 25 και 26 των περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμων του 2001 και 2003. Για τη στοιχειοθέτηση αδικήματος, δυνάμει του πιο πάνω εδαφίου, δεν απαιτείται η ύπαρξη πρόθεσης ή επαγγελματικής αμέλειας.

5.4 Το εδάφιο (3) του άρθρου 10 του περί Επεξεργασίας Δεδομένων Προσωπικού Χαρακτήρα (Προστασία του Ατόμου) Νόμου, αναθέτει στον εκάστοτε υπεύθυνο επεξεργασίας την υποχρέωση για τη λήψη των κατάλληλων οργανωτικών και τεχνικών μέτρων για την ασφάλεια των δεδομένων και την προστασία τους από τυχαία ή

αθέμιτη καταστροφή, τυχαία απώλεια, αλλοίωση, απαγορευμένη διάδοση ή πρόσβαση και κάθε άλλη μορφή αθέμιτης επεξεργασίας. Τα μέτρα αυτά, πρέπει να εξασφαλίζουν επίπεδο ασφάλειας ανάλογο προς τους κινδύνους που συνεπάγεται η επεξεργασία και η φύση των δεδομένων που είναι αντικείμενο της επεξεργασίας.

5.5 Το άρθρο 25 του Νόμου 138(I)/2001, παρέχει στον Επίτροπο Προστασίας Δεδομένων την αρμοδιότητα επιβολής διοικητικών κυρώσεων σε περίπτωση που διαπιστώσει ότι οι υπεύθυνοι επεξεργασίας έχουν διαπράξει παράβαση των υποχρεώσεων τους που απορρέουν από τον Ν. 138(I)/2001.

6. Με επιστολή μου με αρ. φακ. 11.17.001 Α/Π 5/2008 και με ημερομ. 17/1/2008, πληροφόρησα την Αν. Γενικό Διευθυντή Υπουργείου Υγείας ότι αποφάσισα να εξετάσω το παράπονο, το οποίο εκ πρώτης όψεως αφορά παράβαση της υποχρέωσης του αρμόδιου παροχέα υπηρεσιών υγείας για τήρηση και διαφύλαξη ιατρικού φακέλου με βάση το άρθρο 17 του Ν. 1(I)/2005 και την κάλεσα να υποβάλει τα σχόλια/θέση της εντός τριών εβδομάδων από την ημερομηνία της επιστολής. Επειδή δεν έλαβα τα σχόλια της εντός της καθορισμένης προθεσμίας, με την ταυτάριθμη επιστολή μου ημερομ. 22/2/2008 ζήτησα την επίσπευση της υποβολής τους.

7. Δεν υπήρξε οποιαδήποτε εξέλιξη, γι' αυτό με την επιστολή μου με αρ. φακ. 11.17.001 Α/Π 5/2008 και ημερομ. 14/3/2008 πληροφόρησα το Γενικό Διευθυντή Υπουργείου Υγείας ότι αν δεν έχω τα σχόλια του εντός δύο εβδομάδων θα θεωρήσω ότι εξακολουθεί να ισχύει η παραδοχή του (βλ. παρ. 2) ότι ο φάκελος του ασθενούς έχει απολεσθεί και τον προειδοποίησα για το ενδεχόμενο να προχωρήσω βάσει του άρθρου 25 του Ν. 138(I)/2001 στην επιβολή διοικητικής κύρωσης εναντίον του. Παρήλθε και αυτή η προθεσμία άπρακτη και μέχρι σήμερα δεν έχω λάβει οποιαδήποτε σχόλια του καθ' ου το παράπονο. Ως εκ τούτου θεωρώ ότι εξαντλήθηκε κάθε χρονικό περιθώριο για την άσκηση του δικαιώματος προηγούμενης ακρόασης του υπεύθυνου επεξεργασίας πριν από την επιβολή διοικητικής κύρωσης, όπως προνοεί το εδάφιο (2) του άρθρου 25 του Ν. 138(I)/2001.

8. Έχοντας υπόψη όλα τα πιο πάνω και ιδιαίτερα την παραδοχή του Γενικού Διευθυντή Υπουργείου Υγείας που αναφέρεται στην παρ. 2 της παρούσης Απόφασης ότι ο ιατρικός φάκελος του παραπονούμενου κ. Σ.Α. δεν κατέστη δυνατό να ανευρεθεί, με αποτέλεσμα ο παραπονούμενος να μην μπορεί να ασκήσει το δικαίωμα για πρόσβαση στα προσωπικά δεδομένα υγείας του βάσει του άρθρου 18 του Ν. 1(I)/2005 και του άρθρου 12 του Ν. 138(I)/2001, λόγω της παράβασης της υποχρέωσης εκ του εδαφίου (3) του άρθρου 10 του Ν. 138(I)/2001 του υπεύθυνου επεξεργασίας για λήψη των κατάλληλων μέτρων για την ασφάλεια των δεδομένων και την

προστασία τους από τυχαία απώλεια, αποφάσισα βάσει της εξουσίας που μου παρέχει το άρθρο 25(1) του Ν. 138(Ι)/2001 την επιβολή της διοικητικής κύρωσης της χρηματικής ποινής των δύο χιλιάδων ευρώ (€2,000).

Γούλλα Φράγκου
Επίτροπος Προστασίας Δεδομένων
Προσωπικού Χαρακτήρα