EUROPEAN COMMISSION
DIRECTORATE-GENERAL JUSTICE, FREEDOM AND SECURITY

COMPARATIVE STUDY

ON

DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS

Contract Nr: JLS/2008/C4/011 – 30-CE-0219363/00-28

COUNTRY STUDIES

(Douwe Korff, Editor)

A.5 – GREECE

BY

Lilian Mitrou

Submitted by:

LRDP KANTOR Ltd (Leader)
In association with

Centre for Public Reform

(Final edit – May 2010)

GREECE

By Lilian Mitrou

I. Context of information privacy in Greece

1. Political and economic context

In Greece, there is a popular sensitivity and vigilance against any state monitoring and filling. Having the experience of mass surveillance beginning at the Civil War (1946) and till the fall of military dictatorship (1974) many Greek citizens have reproduced a negative surveillance culture and a popular mistrust for any state (and police) surveillance. Greek citizens, deprived for a long time of any political privacy protection for their socio-political views, which were used to classify them as "loyalists" or "enemies" of the state, have learned to mistrust any state personal data collection, even for legitimate purposes [1].

At the same time social analysis, surveys and media reports confirm a "Greek surveillance paradox"[2]: while there is a popular sensitivity, vigilance and resistance against any state monitoring and filling, Greeks show a conspicuous apathy for non-state, private surveillance and data collection. Surveys show that most young Greeks, except their concern against the police cameras, care less for the respect of their communicational privacy (via internet and mobile phone surveillance), provide easily personal data for commercial purposes and enjoy watching Big Brother's type of TV reality shows[3].

There are very few and no specific public opinion pools-surveys concerning the awareness regarding data protection law and rights in the population or in special segments of the society. At the beginning most people were also confused both about the scope and the purpose of the law and about the powers granted to the Data Protection Authority. The initial approach and attitude to the new regulation seemed to be a mixed one: it ranged from indifference to great expectations that the DPA would prohibit the collection and processing of data in general[4]. According to a recent survey[5] concerning the so-called "trust indicator"of public authorities and private organizations, the DPA has acquired an adequate position: with the exemption of the Citizen's Ombudsman, the DPA ranks above other independent authorities[6] as far as it concerns the trust that the citizens have in the Authority.[7] According to another survey (MRB 2007) the DPA has been positioned in second place (after the Citizen's Ombudsman, 50, 3%) in relation to its "recogniseability" (43,6%).

---

1 Samatas points out that this overall anti-surveillance attitude inhibits any state surveillance modernization and efficiency; it also bans surveillance expansion against civil liberties. A negative legacy of authoritarian mass political surveillance has caused a popular demonization of any state surveillance, even for public safety, taxes, or traffic control (Samatas, M. (2010, forthcoming) "Surveillance Legacy, Modernization and Controversy in Contemporary Greece" in L. K. Cheliotis and S. Xenakis (eds) *Crime and Punishment in Contemporary Greece: International Comparative Perspectives*. Oxford: Peter Lang AG.

2 So Samatas.

3 Samatas has conducted such as a survey on " Privacy and Personal Data Protection" (2008) among the students of University of Crete . See summary at *Eleftherotypia*, Febr.2, 2008:54 .

4 See Thematic Legal Study on Assessment of Data Protection Measures and Relevant Institutions – Greece, Report elaborated for the Fundamental Rights Agency by L. Mitrou (2009)

5 About the survey of Public Issue, which takes place every year in December, see www.publicissue.gr

6 Furthermore, it is remarkable that while the DPA enjoys a trust indicator of 130 (2008) or 144 (2007) the Justice Authorities have only 83 (2008) or 84 (2007).

7 For more information see www.publicissue.gr

The interest of people in the data protection framework and the Authority was temporary and it was at a peak when there was some concrete case in the media that caught the public's attention. In fact, the Greek DPA has become broadly known[8] with some famous cases, in which its approaches and rulings have not necessarily gained the support of the majority of the citizens: the Decision of the DPA in relation to Identity cards (15.05.2000)[9] has triggered an extraordinary reaction from the part of the Greek Church, a reaction that has polarized the Greek society and has dominated political life and media coverage for most of 2000 and 2001[10].

2. International obligations in relation to privacy

Greece has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Being a member of the Council of Europe, Greece has also signed the Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data. The Greek Parliament ratified the Convention in 1992 even without having (at that time) data protection legislation in place, i.e. contrary to the respective requirement of the Convention 108.

Greece is a member of the Organisation for Economic Cooperation and Development (OECD) and has adopted the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.

As a Member State of the European Union, Greece has to comply with the privacy and personal data processing and protection legislation adopted on European Union level .

3. Constitutional and common law protections

The Hellenic Constitution (1975/1986/2001) recognizes explicitly the rights of privacy and secrecy of communications. Article 9, initially introduced by the Constitution of 1975, established the protection of privacy in its narrow sense, stating that "every person's home is a sanctuary. The private and family life of the individual is inviolable. No home search shall be made, except when and as specified by law, and always in the presence of representatives of the judicial power. Violators of the preceding provision shall be punished for violating the home's asylum and for abuse of power, and shall be liable for full damages to the sufferer, as specified by law". A new provision granting individuals an explicit right to protection of their personal information has been added by the constitutional revision of 2001. According to Article 9A, "all persons have the right to be protected from the collection, processing and use,

[8] Stavrakakis points out that up to the Identity cards Decision (15.05.00) the DPA was an unknown authority. Y. Stavrakakis, Journal of Modern Greek Studies, 21 (2003), p.153 ff.

[9] The unanimous decision of the DPA was that religious belief, among a set of other sensitive personal data (including fingerprint) should be excluded from identity cards. The Prime Minister C. Simitis confirmed some days later that the Government would implement the decision of the DPA.

[10] The reactions have come down since the appeal of a group of theology professors and laymen against the decision of the DPA was rejected by the Council of State, which ruled that any mention of religion (either obligatory or optional) is unconstitutional. The European Court of Human Rights has also vindicated the Data Protection Authority (ECHR, Sofianopoulos and others vs. Greece, Judgment of 12.12.2002).

especially by electronic means, of their personal data, as specified by law". Article 9A also establishes an independent oversight mechanism providing explicitly that "the protection of personal data is ensured by an independent authority, which is established and operates as specified by law."

Article 19 of the Constitution protects communicational privacy, stating that "secrecy of correspondence and all other forms of free correspondence or communication shall be absolutely inviolable. The guarantees under which the judicial authority shall not be bound by this secrecy for reasons of national security or for the purpose of investigating especially serious crimes shall be specified under law." The 2001 constitutional revision, which added two new provisions to this article, established an independent authority to supervise matters relating to telecommunications secrecy. The establishment, operation and powers of the independent authority ensuring the secrecy of communications are to be specified by law. As additional guarantee against the infringements of the rights to privacy, data protection and freedom of communication, article 19§3 provides that the use of evidence acquired in violation of the present article and of articles 9 and 9A is prohibited.

The general clause of the protection of personality, Art. 57 of the Civil Code can serve (and has served) as grounds of liability for any impermissible processing of personal data. Art. 57 has been applied widely. All the indications from our jurisprudence are clear, that the Greek courts were ready to interpret the clause for the protection of personality as a proper foundation of a cause of action aiming at the prescription of the illegal processing of personal data and, most importantly, at an award for damages for moral harm (non-pecuniary losses) independent from any physical or generally, tangible, injury[11].

II. Legislation

1. The main law

The Greek Data Protection Law of 1997, Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data (hereafter: "the Law") was the first such law introduced in the country.[12] It was also the first law in the EU to be aimed specifically at implementing the Framework Directive on Data Protection *(*Directive 95/46/EC*,* although the Law in various aspects did not conform to the Directive. The provisions of the law cover, without exceptions and without differentiations, automated processing but also processing carried out by conventional means. Law 2472/97 constitutes a framework of rules, which rest on four pillars: a) a system of substantive regulations[13], b) the allocation of rights to individuals, c) the establishment of the Data Protection Authority and d) a system of administrative and penal sanctions as well as provisions on civil liability. The Greek law does not follow exactly the structure of the transposed Data Protection Directive but all of the main provisions of the directive can be found. *Initially, t*he Greek legislator has made full use of the discretion provided by the Directive in order to enhance further the protection of citizens: the law did not introduce the exemptions of Art. 13 of the Directive. Ten years later

[11] So M. Canellopoulou-Bottis, The Implementation of the European Directive 95/46/EC in Greece and Medical/Genetic Data, *European Journal of Health Law* **9**: 207-218, 2002

[12] An unofficial English translation of the Law, can be found on the Greek Data Protection Authority's website: www.dpa.gr/home_eng.htm.

[13] That means the establishment of conditions, obligations and responsibilities for the lawful processing of personal information - followed by the introduction of a quite generalised notification requirement.

(2007), these exemptions have been evoked as the legal ground for the restrictions of the scope of the law introduced through Law 3625/2007.

Partly in order to keep pace with regulatory and technological developments and partly to remedy some deficiencies of the regulatory framework, the Law has been firstly amended in 2000 and 2001. Another amendment of importance was effected through the Law 3471/2006: the scope of application of the law (Art. 3) has been brought in line with the provisions of the Directive 95/46/EC. With the same amendment the notions of the "file" and "sensitive personal data" have been redefined. This amendment has also clarified the competencies of the Authority pertaining to the transborder flow of personal data. An important amendment has been introduced through Art. 8 of the Law 3625/2007. It concerned a) the scope of application of the law, exempting the processing of personal data through judicial authorities, prosecutors and security/police authorities for the purposes of law enforcement from the application of the law provisions, b) the use of CCTV systems for the prevention of disorder and enforcement of crimes committed in the context of demonstrations and c) the provision of information to the media in relation ro criminal proceedings (about suspects, accused or convicted persons). The last amendment of the Law has been adopted by the Parliament on 16.7.09 but the Law has not yet been published.

2. Definitions, Core Concepts and scope

As far as it concerns definitions, most of the basic data protection terms—personal data[14], data subject, controller, processor, third party, recipient and consent—are defined in Art. 2 of the Law generally in compliance with the Directive, but with some modifications. A first derogation refers to the statistical data, where the Law expressly states, in Art. 2(a), that "consolidated data of a statistical nature" are *not* to be regarded as "personal" if the data subjects can *no longer* be identified.

The Law also, in Art. 2(b), adds a definition of "sensitive data." This includes the "special categories of data" listed in Art. 8(1) of the Directive[15], i.e., data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health [16] or sex life. The Greek Law initially included in this category information on membership in a [read: any kind of] society [or] association**"**.[17] According to

[14] As expressly confirmed by the Greek DPA in many decisions and directives concerning surveillance through CCTV systems, sound and image data are deemed to be "personal data" if they can be linked to identifiable individuals, as will be the case if such data are stored and further processed: "Storage and transmission of images of an individual, recorded by a fixed closed circuit television, operating on a regular, continuous or permanent basis, outdoors or indoors, such as on streets, squares, stations, ports, stadia, in banks, stores, theatres, cinemas, or public transportation means, constitute processing of personal data, in the terms of [the Law]", see Data Protection Authority, Directive 1122 of 26 September 2000 on the use of close-circuit television systems.

[15] The definition adopted is also influenced by the respective provision of Convention 108 of the Council of Europe.

[16] It may be noted with regard to genetic information that (although the Data Protection Authority accepts that it is difficult to classify such data precisely), such information is always "sensitive" because it relates, especially, to health, race and ethnic origin. See Decision 15-2002 of 15 February 2001 on "*DNA analysis for the purpose[s] of criminal investigation and penal prosecution.*"

[17] Information on membership in organizations other than trade-unions is not regarded as "sensitive" at all in the Directive (unless such membership "reveals" a person's religious or philosophical beliefs).

the revised definition (through Law 3471/06) "sensitive data" shall mean the data referring to racial or ethnic origin, political opinions, religious or philosophical beliefs, membership to a trade-union, health, social welfare and sexual life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas. The Law also includes in the general concept of "sensitive data," information on criminal charges or convictions[18].

A further derogation concerned the term "(personal data) file" was initially (1997) defined in Art. 2(e) as "any *set* of personal data which are or may be processed" by any kind of controller. The initial definition of the "filing system", which meant as such any set of personal data has been considered (even by the Authority) as "too wide". As file is now (since 2006) defined "any structured set of personal data which are accessible on the basis of specific criteria", a definition closer to this adopted by Directive 95/46/EC. It is noteworthy that the Greek law contains a specific and separate definition and regulation of the so-called "interconnection of files", which is meant as the linking of *either* a computer or filing system controlled by one controller to a computer or filing system controlled by a different controller, *or* of two computers or filing systems controlled by the same controller, if the two systems were established for different purposes.

Slightly different defined is also the term of data subject's consent: in accordance with the Directive the Law lays down a number of elements that effectively amount to the required conditions for valid consent[19]. However, the Greek Law adds a) a list of the information to be provided in order to meet the "informed" requirement and b) the right to revoke consent "at any time without retroactive effect." (Art. 2(k)).

The Greek legislator opted for a general legal framework with a wide scope including all relevant areas of society (the so-called "omnibus-approach"). The Greek system could also be described as "monistic", in the sense that consolidated rules on data processing are introduced both regarding the private and the public sector[20].he Law applies to all processing of personal data by (wholly or partly) automatic means as well as to the processing of such data by means of non-automatic "files" (i.e., by means of "structured" manual data sets) (Art. 3(1)). Since the concepts of "personal data" and "data subject" are limited to natural persons, this means that the Law does *not* apply to "legal persons" or deceased persons.

3. Exemptions

In accordance with Art. 3(2), second indent, of the Directive, the Greek Law contains a general exemption, with regard to "processing by a natural person in the course of a purely personal or household activity" (Art. 3(2)). It is worthy to mention that the Law did *not* contain full, or even very wide, exemptions with regard to matters such as national security, defence, police or other criminal-legal matters, or the like (the more limited exceptions, e.g.,

[18] Information on criminal-legal matters is considered a "special category of data" in the Directive, but is treated differently from the other "special categories." However, by including those data in the general definition, the Greek Law makes the processing of criminal-legal data subject to the same rules as the processing of the other kinds of "sensitive data".

[19] These are that the consent must have taken the form of a "freely given, specific and informed" expression of the will of the data subject, through which he or she agrees to the (specific) processing in question..

[20] Thematic Legal Study on Assessment of Data Protection Measures and Relevant Institutions – Greece, Report elaborated for the Fundamental Rights Agency by L. Mitrou (2009)

as concerns the exercise of data subject rights, will be noted in the appropriate sections where relevant). Such an exemption has been introduced through Art. 8 of the Law 3625/2007, exempting the processing of personal data through judicial authorities, prosecutors and security/police authorities for the purposes of law enforcement from the application of the law provisions and the oversight of the Data Protection Authority. The recently adopted (July 2009) amendment exempts the use of CCTVs in public places from the scope of application of the Data Protection Law and accordingly from the oversight through the Data Protection Authority. The exclusion of the processing of the personal data by the police and in general the security authorities from the scope of application of the Law and the monitoring through the Data Protection Authority as well as the recent amendment of the law has raised a vital public and scientific discussion and protest from media, NGOs and political parties. According to legal doctrine these amendments ignore the so-called "shield function" of the data protection legislation and the data protection authority, which offers an adequate guarantee for the citizens against the misuse of his/her data by police and other security authorities. Taking into account that the right to data protection is to be ensured by an independent authority, which is the sole competent for monitoring enforcement, is explicitly embedded in the Greek Constitution (art. 9 A), the new provision raises significant concerns in relation to its compliance with the Greek constitutional framework[21]. The Data Protection Authority in two opinions published at the end of July 2009[22] has characterized the law amendments introduced as unconstitutional. The Authority has also pointed out that these amendments infringe also Art. 8 of the European Convention on Human Rights as interpreted through the jurisprudence of the European Court on Human Rights.

A further concern relates to the processing related to the press or to the more general exercise of freedom of expression. With regard to the wide exemptions provided by the Directive in Art. 9 the Greek Law provides only for an exemption from information duties: Art. 11(5) exempts the press from the duty to inform data subjects, and even then only if the data subjects are "public figures". The Law also allows for the processing of sensitive data of "public figures" for journalistic purposes**,** but only on the basis of a special permit, to be issued by the Data Protection Authority. However, it is noteworthy that the provision concerning the permit to be issued for the lawful processing of sensitive data of public figures has till now never been applied and enforced by the Greek DPA[23].

4. Territorial scope

With regards to the territorial scope the Law stipulates that it applies to all processing by a controller established on the territory of Greece (or otherwise subject to Greek law "by virtue of public international law," e.g., to ships flying the Greek flag or Greek embassies) (Art. 3(3)(a)). This provision is basically in compliance with the Directive, except that the latter refers, somewhat more specifically, to processing "carried out in the context of the activities

[21] For an analysis of the new provisions and its constitutional implications see the collective work "The electronic surveillance in public places" (in Greek), Athens-Thessaloniki 2008.

[22] Data Protection Authority, Opinion 1/2009 on the Law amendment concerning the use of CCTVs in public places and Opinion 2/2009 concerning the DNA Databank for security and law enforcement purposes.

[23] The Greek DPA has imposed sanctions on media enterprises and journalist. However the legal ground for the imposed sanctions has been till now the infringement of the proportionality principle by processing of personal data. The Council of State (the Greek Supreme Administrative Court) has confirmed in several rulings the right of the Authority to assess the processing of personal information for journalistic purposes under the criteria of data protection legislation.

of an establishment of the controller," when that "establishment" is situated on the territory of the Member State in question(Art. 4(1)(a) of the Directive). In the case that processing is carried out by a controller who is "*not* established in the territory of a member-state of the European Union but in a third country" (Art. 3(3)(c)), the Greek Law provides, in accordance with Art. 4(1)(c) of the Directive, that it shall apply to such processing if "for the purposes of processing personal data, [the controller] makes use of equipment, automated or otherwise, situated on the Greek territory, *unless* such equipment is used only for purposes of transit through such territory."[24] In this case the non-EU controller has to appoint a "representative" in Greece. This appointment must be made "in writing" by means of a statement to the Greek Data Protection Authority. The representative will be subrogated in all the rights and duties of the controller, without prejudice to any legal action which can be taken against the controller himself.

Another provision, dealing with application of the law in the case of controller who is "not established in Greek territory or in a place where Greek law applies, when such processing refers to persons established in Greek Territory." (Art. 3(3)(b)), was extensively criticised with regard to its compliance with the Directive, as it could be seen as a "restriction" (in the form of a "formality") affecting the free flow of personal data between the EU Member States, in contravention of the fundamental principle establishing a "free zone" for intra-EU data transfers, stipulated in Art. 1(2) of the Directive.[25] This provision has been abolished through Law 3471/06 in order to bring the Greek law in line with the Directive.

5. Other legislation relevant to data protection

Law 2472/97 has been initially complemented by Law 2774/99 on the Protection of Personal Data in Telecommunications Sector[26]. Law 2774/99 has been amended by the Law 3471/06 in order to harmonize the respective Greek framework with the Directive 2002/58/EC. The Law 3471/06 contains provisions relating to the secrecy of electronic communications services, the processing of traffic data, the itemized billings, the identification of calling-connected line, the directories of subscribers and the unsolicited calls. The Greek legislator has also introduced general principles concerning the fair and lawful processing of personal data in the electronic communications sector: a) explicit prohibition of secondary use unless the subscriber has provided explicit and specific consent, b) detailed information duties of the providers, c) introduction of "privacy by design" and the so-called "data sparing principle"[27] and d) possibility of anonymous use and payment of electronic communication services. This latter right (d) has been seriously restricted through a recent act, adopted in July 2009 by the Greek Parliament, which prohibits the anonymous provision and use of mobile phones, in order to enhance security and law enforcement.

---

[24] It is proposed that the words "transit through such territory" must be interpreted , in accordance with the wording and the purposes of the Directive, as referring to transits of data through the territory of the European Community (and not just to transit through the territory of Greece).

[25] The European Commission in its contacts with Greece (2003) has stressed this point as especially problematic with regard to compliance with the Directive.

[26] This Act had transposed the Directive 97/66 concerning the processing of personal data and the protection of privacy in the telecommunications sector into Greek law.

[27] According to Art. 5 § 6 the technical means, IT systems and the equipment for the provision of electronic communication services should be designed and selected in such way that they fulfil their purpose using the minimum possible data. This provision reflects not only the support of Privacy Enhancing Technologies but also the specific preference for the so-called data sparing approach.

Apart from the abovementioned laws there are no sectoral laws pertaining to the processing and protection of personal data. References in specific laws relate merely to the need to take into account the requirements of the Law 2472/97 when processing personal data in specific contexts. Such cases concern the processing of personal data in relation to a) digital/electronic signature services[28], b) the re-use of public sector information[29] or c) the processing of data for the prevention and detection of organised crime[30], d) the processing of health data by health professionals, who are obliged to process the said data in a way to ensure medical secrecy and the data protection[31].

6. The data Protection Principles

General considerations

The data protection principles, contained in Art. 6 of the Directive, are set out in very similar, but not quite identical, terms in Art. 4 of the Law (under the rather confusing title "Characteristics of Data Processing). According to the law, personal data must be processed "fairly and lawfully" and for "specific, explicit and legitimate purposes" (Art. 4(1)(a)). In accordance with the Directive, the Greek law stipulates that personal data must be "adequate, relevant and not excessive in relation to those purpose (Art. 4(1)(b)), as well as "accurate and, where necessary, kept up to date" (Art. 4(1)(c)). The principle of proportionality is a key feature of the data protection law and especially of the jurisprudence of the DPA[32] in Greece.

'Purpose-limitation principle'

According to the Law data must be "collected fairly and lawfully for specific, explicit and legitimate purposes". A difference between the Greek Law differs and the Directive's provision concerns the purpose limitation principle. The Directive adopts the "purpose-limitation principle" providing that personal data may *not* be further processed "in a way incompatible with [the specified purpose for which the data were obtained] (Art. 6(1)(b)). The Greek Law however says that personal data, must be processed "fairly and lawfully...in view of such purposes" (Art. 4(1)(a)). The Authority conceives the purpose-limitation principle in a flexible and open way. Both in the interpretation of the Law as well as in the jurisprudence of the DPA reference is made not only to the criterion of "fairness" but also – and perhaps mainly - to the "compatibility" of further processing with the primarily defined purpose.[33]

Explicitly, the Greek Law considers "further processing of data for historical, statistical or scientific purposes" neither as compatible nor as incompatible[34]. The law does not prohibit

[28] Art. 7 of the Presidential Decree 150/2001 concerning electronic signatures

[29] Art. 3§ 2 of the Law 3448/06 concerning the re-use of public sector information.

[30] Art. 6 of Law 2928/2001 concerning the amendments of Penal Code and Penal Procedure Code for the protection of citizens with regard to organised crime.

[31] Art. 13 and 14 of the Code of Conduct for Health Professionals (Law 3418/2005)

[32] Many (famous) decisions of the Authority refer to the proportionality principle, which has been the main criterion for assessing the lawfulness of the processing in various sectors and contexts (Identity cards decision, decisions referring to biometric identification of employees or air passengers, decisions referring to the use of CCTVs in public and private places) .

[33] See Decisions about the use of a videotape containing a surgery, recorded for

[34] The Directive says that data shall not be kept in identifiable form for longer than necessary (for either the primary or any legitimate secondary purpose for which they are processed), and that Member States must

principally such uses. It introduces as "appropriate" safeguard the permit of the DPA, which may allow further retention and "secondary" use for historical etc, purposes. Further processing for such purposes is associated in Greek Law with the question of lawful retention of data. On data retention, the Greek Law, by seemingly contrast to the Directive, implies that personal must be kept in a form permitting the identification of data subjects for the period necessary, according to the assessment of the Greek Data Protection Authority, with reference to the purposes for which the data were collected or are further processed (see Art. 4(1)(d), first sentence, of the Law). However, this provision has not be interpreted in the sense that the maximum retention period for personal data is to be specified by the Greek Data Protection Authority. Its meaning lies in the possibility of the Authority to assess the processing period and practices as defined by the Data Controller and impose restrictions and modifications in accordance to its power to intervene in order to ensure compliance with the data protection principles.

Criteria for lawful processing

As concerns the criteria for legitimate processing of personal data , Article 5 of the Law sets out the criteria contained in Art. 7 of the Directive, however with some significant differences. The first point of difference concerns the "consent" of the data subject. The Greek data protection law places particular emphasis on the "consent" of the data subject to the processing of his/her personal data: In the Greek Law consent serves as the standard norm and all other legal grounds (contract, legal obligation, vital interest, public interest, lawful interest of data controller/third person) are considered as exceptional. This provision, which deviates from the choices of the EU legislator who regarded consent as one of the several legal grounds for lawful processing (Art. 7 of the Directive 95/46/EC), was adopted under the pressure of several MPs who wished to manifest the priority to be given to the self-determination of the individual[35].

The Greek Data Protection Authority is very strict with regard to consent. Applying the detailed definition of consent as well as the general principles of Greek constitutional and civil law the DPA has ruled that consent is void, if that is contra bonos mores or public order (in the sense of *ordre public*), or that would lead to a violation of the data subject's fundamental rights. According to the Authority such a case was the case of consent given by volunteers locked up in the "*Big Brother House" (2001).* Especially in the case of processing of employees's/workers' personal data the Data Protection Authority does not accept [36]in principle the "consent" as a legal ground for collection and processing, as it doubts if such a consent is "free", as required by definition of consent (Art. 2 k of Law 2472/97).

Another derogation from the Directive concerns the so-called "balance" (of interests) criterion. In the Directive this criterion allows for processing which is "*necessary*" for the "legitimate interests" of the controller (or indeed for the legitimate interests of a third party), except where such interests are "overridden by the [data protection] interests of the data subject." (Art. 7(f)). By contrast, the Law allows processing if "the processing is ***absolutely*** *necessary* for the purposes of a legitimate interest pursued by the controller or a third party or third parties to whom the data are communicated and on condition that such a legitimate

provide "appropriate safeguards" with regard to processing for historical, statistical or scientific purposes.

[35] See Proceedings of the Debate in the Plenary Session of the Greek Parliament of 13 March and 18 March 1997.

[36] See Decision 115/2001 "Guidelines for the protection of personal data in the employement context"

interest ***evidently*** prevails over the rights and interests of [the data subjects] and that their fundamental freedoms are not affected" . As noted, this quite clearly is a much more "weighted balance" test, with the scales quite decisively tilted towards the data subject.

Data security obligations

In accordance with the Directive (Art. 16 and 17) The Greek law contains ignificant requirements for the *confidentiality* and *security* of data processing (Art. 10). Art 10 provides that processing is confidential and it has to be conducted by persons acting under the authority of Data and upon the instructions of Data Controller and Data Processor. The Greek Authority puts specific importance on data security measures[37]. Upon proposal of the DPA the amendment of 2006 (Law 3471/06) has recognized explicitly the competence of the Authority to issue guidelines and instructions concerning the level of security of data and of the computer and information infrastructure, the security measures that are required for each category and processing of data as well as the use of Privacy Enhancing Technologies.

Deletion of data

As mentioned above the Law provides that personal data must be kept in a form which permits identification of data subjects for no longer than the period required for the purposes for which such data were collected or processed. Once this period of time is lapsed, the Authority may, by means of a reasoned decision, allow the maintenance of personal data for historical, scientific or statistical purposes, provided that it considers that the rights of the data subjects or even third parties are not violated in any given case.

The Law furthermore stipulates that any personal data that are, or have been processed, contrary to the quality requirements of the law (i.e., which are irrelevant, excessive, inaccurate, or outdated, or which are processed unfairly or unlawfully) must be destroyed, such destruction being the Controller's responsibility. This requirement goes beyond the respective provision of the Directive that merely stipulates that the controller must take "every reasonable step...to ensure that data that are inaccurate or incomplete...are erased or rectified." (Art. 6(1)(b), second sub-clause).

7. Areas of special concern

Processing of Sensitive Data

The processing of any of the above kinds of sensitive data is regulated in Arts. 7 and 7*a* of the Law in a more restrictive way, than is the processing of the more limited kinds of "special data" in the Directive. Processing of sensitive data is principally prohibited but the law foresees derogations from this prohibition in a number of special cases laid down in Law and under the (procedural) condition that the Data Protection Authority has issued a permit for the processing in question (Art. 7(2), initial sentence). The circumstances in which processing of

[37] The Greek DPA has imposed several sanctions for lack or infringement of data security services. The Authority has issued specific guidelines for the secure deletion and destruction of data and files. It is also noteworthy that the Greek DPA requires a data security plan in order to issue a permit for the processing of sensitive data.

sensitive data is allowed with a permit**,** or rather, in which a permit may be issued , are first of all the following:

a) written consent of the data subject:[38]

b) processing is necessary to protect the vital interests of the data subject or the interests of a third party provided for by the law, if s/he is physically or legally incapable of giving his/her consent (Art. 7(2)(b));[39]

c) the processing relates to data made public[40] by the data subject or is necessary for the establishment, exercise or defence of rights in a court of law or before a disciplinary body;[41]

d) the processing is necessary for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, provided the processing "relates to" health matters and that the processing is carried out by a health professional subject to the obligation of professional (medical) secrecy or relevant codes of conduct.

A permit of the DPA is also required[42]:

a) if the processing is carried out by a public authority and is necessary for the purposes of national security, or for purposes of criminal or correctional policy (provided it pertains to the detection of offences, criminal convictions or security measures), for public health purposes or for the exercise of public control on social welfare services (Art. 7(2)(e));

b) if the processing is carried out exclusively for research and scientific purposes provided that anonymity is maintained and all necessary measures43 for the protection of the persons involved are taken (Art. 7(2)(f));

---

38 Unless such a consent has been extracted in a manner contrary to the law or *bonos mores* or if [a] law provides that any consent given may not lift the relevant prohibition" (Art. 7(2)(a))

39 Initially there was no provision concerning the vital interests of "another person". This case was enacted through the amendment of Law 3471/06.

40 It is noteworthy that the Directive requires that the data must have been "*manifestly*" made public by the data subject.

41 The Greek Law expressly includes the establishment, exercise and defence of rights also in *disciplinary bodies*. Even if this case is not explicitly included in the Directive, in terms of the Directive disciplinary proceedings can usually be considered to be included in the concept of proceedings relating to "*legal claims*" at least if the disciplinary bodies have been established by, or are otherwise recognised in, law.

42 These cases, included in Greek Law, are *not* expressly foreseen in the Directive. However, as noted by Korff, they can be brought under the more general exception in Art. 8(4) of the Directive, which allows for the granting of additional exemptions from the in-principle prohibition on the processing of sensitive data "for reasons of *substantial public interest***,**" either by national law or (as is the case here) "by decision of the supervisory authority," provided "*suitable safeguards*" are laid down for the processing in question.

43 The DPA may assess the measures provided by data controller or/and set out additional measures in order to preserve anonymity or the respect of fundamental rights and freedoms of the data subject and/or third parties. There is a number of decisions of the DPA concerning the historical research with regard to the period of Second World War (and mainly the case of "collaborators" of the occupation forces) and the Greek Civil War (1946-1949). The approach of the DPA has however been criticised as "research-restrictive".

c) if the processing carried out refers to sensitive data on public figures, for journalistic purposes, provided that such data are in connection with the holding of public office or the management of third parties' interests, and only if such processing is absolutely necessary in order to ensure the right to information on matters of public interest.

In respect of c), the law adds that a permit may also be issued in connection with literary expression, and that processing can be carried out under the permit, provided the right to protection of private and family life is not violated in any way whatsoever (Art. 7(2)(g)). However, as mentioned above, this provision (Art. 7(2)(g)) is widely considered as unconstitutional and has never been neither applied by the Authority nor assessed by Courts.

The Greek law provides for processing of sensitive data without a notification/prior notification (and permit of the DPA) is allowed in a limited number of cases, which partly correspond to some of the other special exceptions in the Directive. These cases were introduced through amendments of the law, mainly this of 2000, in order to face the problem of "notification flood". Processing is exempted from notification and prior notification in the following cases:

a) if it relates directly and exclusively to an employment or similar relationship, and is necessary for the fulfilment of an obligation imposed by law or arising out of the employment (or similar) relationship (and on the further condition that the data subject was informed of the processing in advance) (Art. 7a(1)(a)). The requirement to inform the employee-data subject as well as the emphasis on the requirement for the processing to be directly and exclusively necessary for the specific employment purpose respond to the requirement of the Directive that Member States provide "adequate safeguards" concerning processing "in the field of employment law" (Art. 8(2)(b));

b) if it relates to personal data on *clients or suppliers, pro*vided that such data are *neither transferred nor disclosed to third parties (Art*. 7*a*(1)(*b*), first sentence). This exception does not apply to: insurance companies, pharmaceutical companies, companies, whose main activities involve trading of data (i.e., list brokers), credit and financial institutions (such as banks and institutions issuing credit cards);

c) if it is carried out by *societies, enterprises, associations or political parties and r*elates to personal data on their *members or associates, pro*vided that the latter have given their *consent and* that such data are *neither transferred nor disclosed to third parties (Art*. 7*a*(1)(*c*), first sentence)[44]. This exemption relies on the emphasis given on consent as well as to the requirement to respect the collective autonomy of such organisations and their position in constitutional framework. The importance of the provision here is that associations, etc. do not need to obtain a *permit to p*rocess data on their members. A *transfer of me*mbers' or associates' data to *other members or associates is not* to *b*e considered a transfer to "*third parties," pro*vided the transfer "is carried out among said members and partners for the purposes of the aforementioned legal entities or associations";[45]

[44] This exception corresponds to the one set out in Art. 8(2)(d) of the Directive - except that in the Directive, that exception is limited to such processing by *not-for-profit body with a political, religious or trade-union aim*.

[45] This is a very tricky question relating to the issue, the boundaries, the conditions and the restrictions of

d) if it is carried out by doctors or other persons rendering medical services and relates to medical data, provided that the controller is bound by a duty of medical confidentiality or other obligation of professional secrecy, imposed by law or by means of a code of practice, and provided the data are neither transferred nor disclosed to third parties (Art. 7a(1)(d)). However, the law provides that organisations rendering health care services, such as clinics, hospitals, medical centres, recovery and detoxification centres, insurance funds and insurance companies, as well as controllers processing personal data within the framework of programmes of telemedicine or provision of health care services via telematic networks are not exempted from the prior notification/permit requirement;

e) if it is carried out by lawyers, notaries, unpaid land registrars or court officers and relates to the provision of legal services to their clients, provided that the controller is bound by an obligation of confidentiality imposed by law and that the data are neither transferred nor disclosed to third parties, except for those cases where this is necessary and directly related to the fulfilment of a client's mandate (Art. 7a(1)(e)).

The Law also adds, in two of the above-mentioned cases (transfers of data on clients or suppliers, and to the transfer of membership data by associations) that "[transfers of sensitive data to] courts of justice and public authorities are not considered to be [transfers to] third parties, provided that such a transfer or disclosure is imposed by law or a judicial decision." This provision corresponds to the stipulation in the Directive that "authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients" (Art. 2(g) of the Directive).

Automated decisions

The Greek Law contains specific safeguards with regard to the taking of *fully automated decisions based on a personality "profile."* By contrast to the Directive's provision, which recognize persons the right *not* to be subjected to such a decision, if the decision has "legal effects" or otherwise "significantly affect" them[46], the Greek law grants any person the right to "request from the competent court the *immediate suspension or non-application* of *any act or decision* affecting him, based solely on *automated processing of data intended to evaluate his or her personality* and especially his or her effectiveness at work, creditworthiness, reliability and general conduct." (Art. 14(1)). This right applies with regard to the taking of such decisions by administrative authorities, public law or private law entities or associations and natural persons alike (*idem*). The right can be exercised "even when the other substantive conditions for provisional judicial protection" (i.e., for injunctions) do not apply (Art. 14(2)), i.e., there does *not* have to be any illegality or impropriety involved in the decision. It suffices that the decision was a purely automated one and involved an "evaluation" of the data subject's personality or conduct[47].

---

political marketing.

[46] According to the Directive, (Art. 15) such decisions may however be *allowed* if they concerned a *request* by the data subject for the entering into a *contract* and that request was "*satisfied*" *or* there were "*suitable measures to safeguard [the data subject's] legitimate interests,*" such as "arrangements allowing him to put his point of view"; *or* if the decision was *authorised by law* (provided that that law also laid down appropriate "*safeguards*")

[47] Despite the rights provided for persons there is no case publicly known, where this provision has been applied.

Interconnection of files

In accordance with the Directive, which expressly allows Member States to designate other kinds of processing as "operations likely to present *specific risks* to the rights and freedoms of data subjects," and to subject such processing operations to a "*prior check*" (Art. 20), the Greek law requires any such controller or controllers to **notify** any interconnections of files[48] specifically to the Data Protection Authority, and the Authority maintains a special file on such interconnections (aptly called the "interconnection register") which is open to the public (Art. 8(2) and (6)). A permit has to be issued, if one or more of the "linked" files contains *sensitive data* (or if the interconnection results in the disclosure of any sensitive data) *or* if a "uniform code number" is to be used in the interconnection (Art. 8(3).

Direct marketing

There is no specific regulation with regard to processing for the purposes of direct marketing[49]. However, in accordance with its competence to issue instructions for the interpretation and the application of the Law rules, the Greek Data Protection Authority has issued guidelines, stipulating more specific conditions for the lawful processing of personal data for marketing purposes (direct marketing and advertising)[50] .

According to the Authority's guidelines, collection of personal data for the purpose of *direct marketing* and/or *sales promotion* can be carried out *either* with the *prior consent* of the data subject *or* – in absence of consent- on the basis of [data from] *published directories* such as telephone directories and trade fair catalogues, provided that the subjects have *consented* to the inclusion of their data in the said [directories or] catalogues, or have published their data for similar purposes. The Authority considers as lawful also the collection of personal data [for direct marketing and sales promotion] if the said data are collected from *sources available to the public*, provided that any *conditions* regarding lawful access [to such sources] are adhered to. The DPA specifies also the categories of data that may be collected in such cases: they may may include only [the data subjects'] full *name, address and profession*. Furthermore, the DPA requires that "as soon as the *first letter* [sent for the purpose of direct marketing or sales promotion] is sent to the data subject, the sender shall *inform* the addressee of the *source* of his or her information and *ask* for the data subject's *consent* in order to use [read: continue to use] the data.".

In addition, the Authority has issued a Directive setting out conditions on the collection and use of personal data on mothers in maternity hospitals for the purposes of direct marketing or

---

[48] The term applies to either the linking of two or more files (read: automated or manual filing systems) held by two different controllers, or the linking of two or more files (filing systems) held by the same controller, but where the different files or systems that are connected serve different purposes. The DPA considers the online access to a file as a form of interconnection of files.

[49] The Consumers' Protection Law (Law 2251/1994) included before its amendment some provisions concerning the collection and use of publicly available data for marketing purposes. The Consumers Protection Law stipulated also that marketing practices should respect the private life of individuals, a provision inspired by the Council of Europe Recommendation on the use of personal data for direct marketing purposes.

[50] Greek Data Protection Authority Decision No. 050 of 20 January 2000, containing "Conditions for the lawful processing of personal data as regards the purposes of direct marketing/advertising and the ascertainment of creditworthiness," published in abbreviated form in English on www.dpa.gr (website of the DPA)

advertising.[51] In this Guideline, the Authority assesses the quality of consent as a ground for processing and holds that consent to use of (mothers and babies') data for marketing, obtained within a few days after the birth of a baby, was *not* valid in terms of the Law, and that such consent should therefore be sought in a different way, through forms issued through the hospital, when the women left the maternity hospital.

Credit reporting

There is neither specific regulation for credit reporting/referencing. The decision 50/2000 concerned not only the specific requirements for lawful direct marketing but it deals also with direct marketing, also addresses processing of personal data for the purpose of assessing someone's financial standing, i.e., for credit referencing. The Authority aimed at setting conditions in order to reduce processing that takes place without the consent of the subject and avoiding the creation of "overall financial profiles" of individuals without their knowledge.

According to the mentioned Decision, the collection and retention, by companies, etc., of certain basic, unfavorable data, (i.e., information on bankruptcies and petitions for bankruptcy, forced sales of property, information on [a person's interests in] companies and other legal entities and changes in such entities, mortgages, seizures and dishonored checks, etc.) is allowed principally, subject to certain time limits to be set by the Authority and provided the settlement of debts is "immediately" added to the information.Companies keeping records of such matters are required to inform the data subjects of such processing; and they may not add "favorable" financial information (such as information on real estate owned by the data subject) without the consent of the data subject because that would lead to the creation of "overall financial profiles."

The Internet

The Greek Law does not make any special provision with regard to the Internet but there has been no doubt that the Law applies also to activities involving the Internet. Controllers are subject to their information duties (according to Art. 11 of the Law)[52] and they have to clarify whether the providing of the information is *voluntary or obligatory* and if the latter, on the basis of what legal provision the information is demanded. In case of collection of data by means of cookies, Law 3471/06, regulating the protection of personal data in the electronic communications sector, requires explicitly (Art. 4 (5)) that the user is informed according to the requirements of Art. 11 of the Data Protection Law (Law 2472/97) and entitles the DPA to issue specific instructions and guidelines concerning the content and the way this information is to be provided.

[51] Directive 523-18 of 25 May 2000, containing "*Conditions for the lawful processing of personal data of mothers in maternity hospitals for the purposes of direct marketing or advertising*."

[52] Controllers and web hosts should *inform* the visitors to their site of their *right of access* and, if they ask the visitor to provide data on himself or herself (e.g., if they ask him or her to type in their email address), they must *inform* the visitor of *all their rights* (including the right to object to direct marketing use of their data), *in writing*.

8. Cross-Border Data Transfers

The Greek Law expressly stipulates that transfers of personal data to *other Member States of the EU* are *permitted* (Art. 9(1), first sentence). With regard to all other transfers (i.e., to any non-EU States), the Law follows the approach of the Directive. The Law, in Art. 9, allows for such transfers in *substantially the same circumstances*, but subject to an overall requirement that, *for all transfers to non-EU Member States*, a *permit* is required, which can be issued by the Data Protection Authority. Thus, data may be transferred to *non-EU States* (with such a permit) if *the Authority* "*deems* that the country in question ensures an *adequate* level of protection" (Art. 9(1), second sentence). The Law did *not* refer explicitly to the possibility of "findings" being made by the European Commission to the effect that the law in a third country *is* "*adequate*" (as has been done in respect of Switzerland and Hungary) (see Art. 25(6) of the Directive). After the amendment of the Law in 2006 it is explicitly provided that a permit is not required a) if the European Commission has decided, on the basis of the process of article 31, paragraph 2 of Directive 95/46/EC that the country in question guarantees an adequate level of protection, in the sense of article 25 of the Directive or b) if the European Commission has decided, on the basis of article 26, paragraph 4 of Directive 95/46/EC, that certain conventional clauses offer adequate safeguards for the protection of personal data.

The "*derogations*" listed in Art. 9(2) of the Law also in *substance* correspond to the ones set out in Art. 26 of the Directive. These derogations concern

a) The consent of data subject to such transfer. The Law, in line with its general strictures on consent, adds explicitly that this does *not* apply if "such consent has been *extracted* in a manner *contrary to the law* or *bonos mores*";

b) The protection of a *vital interests* of the data subject, *provided he or she is physically or legally incapable of giving his or her consent*;

c) The conclusion and performance of a *contract* between the data subject and the controller (or between the controller and a third party in the interest of the data subject, *if the data subject is incapable of giving his or her consent*), or for the implementation of *precontractual measures* taken in response to the data subject's request;[53]

d) An *exceptional need* and safeguard of an *important public interest*, especially for *the performance of a cooperation agreement with the public authorities of the other country*, *provided* that the controller provides *adequate safeguards* with respect to the protection of privacy and fundamental liberties and the exercise of the corresponding rights;

e) The establishment, exercise or defence of a *legal claim*;

[53] The main part of this derogation corresponds to the one set out in Art. 26(1)(b) of the Directive, but the proviso stipulated with regard to the derogation concerning contracts concluded between others than the data subject "in the interest of the data subject" (placed in brackets above), i.e., that such transfers are only allowed if the data subjects was "incapable of giving his or her consent" is *not* contained in the corresponding provision in the Directive, Art. 26(1)(c)). This can cause problems in connection with credit card payments and the like for which purpose the derogation was added to the Directive.

f) the transfer from a *public register* that by law is intended to provide information to the public and that is accessible to the public or to any person who can demonstrate a legitimate interest, provided that the conditions set out by law for access to such register are fulfilled in each particular case.

The "*derogations*" listed in Art. 9(2) of the Law also in *substance* correspond to the ones set out in Art. 26 of the Directive. In all cases it is the DPA (rather than the controller), which assesses the applicability of a derogation and issues a respective permit.

9. Rights of Data Subjects

Informing of Data Subjects

Art. 11(1) of the Greek Law stipulates that the controller must, *during the stage of collection of personal data*, *inform* the data subject "in an *appropriate* and *express* manner" of a) his or her *identity* and the identity of his or her *representative*, if any,b) the *purpose* of data processing, c) the *recipients* or the *categories of recipients* of the data and d) the existence of the *right of access* to the data.

The Law requires the controller, when asking the data subject to provide the data him- or herself, to *inform* him or her "*specifically and in writing*" of the above, and of *all* the data subject's rights (i.e., not just of the *right of access*, but also of the *general right to object to processing*, and of the specific *right to object to direct marketing use of his or her data*). In additional the controller must also inform the data subject whether he or she is *obliged* to assist in the collection of data, and if so, on the basis of which *legal provisions*, as well as of any *sanctions* resulting from the data subject's failure to co-operate (Art. 11(2)). If the controller obtains the data from *sources other than the data subject*, it would appear that the data subject must be informed of the above still *at this stage of data collection*, and in any case *before any disclosure of the data*.

Exempted[54] from information duties are

a) the case that data are collected for journalistic purposes, if the data relate to *public figures,* and

b) *the case that* processing is carried out for reasons of *national security* or "for the detection of *particularly serious crimes.* In the last case (b) the exemption is applied on the basis of a specific *decision* to be taken by the Data Protection Authority or in case of emergency by the President of the Data Protection Authority**,** who has then to seek the approval of the measure by the members of the Authority "*as soon as possible*" (Art. 11(4)).

[54] The Law does *not* contain the exception from the duty to inform, contained in the Directive, which exempts the controller for his duty to inform the data subject, if the data subject "*already has*" the information (see the introductory sentences to Art. 10 and Art. 11(1) of the Directive).

Confirmation of processing

The Law extends the right to obtain *confirmation*, *on request*, of *whether personal data* relating to the data subject *are being processed*[55], to the right to obtain information also on whether such data *have been processed*. The Law requires that the reply must be made *in writing* (Art. 12(1)).

Access

If data are being processed on him or her, the data subject has a *right of access*, i.e., the right to obtain from the controller, "without undue delay and in an intelligible and express manner," the following information: a) all the *personal data relating to him* that are still held by the controller, as well as their *source*[56], b) the *purposes* of data processing, c) the *recipient* or the *categories of recipients*, d) any *developments* as to such processing for the period since the data subject last exercised his or her right of access and e) the *logic* involved in the *automated data processing*.

The requirement that the controller must inform data subjects of any *developments* as to the processing of their data since they last exercised their right of access, is an additional requirement in relation to these of the Directive. Beyond the requirement in the *Directive* is also the provision of the Law, that grants data subjects the right to be informed of the "*logic*" involved in the (i.e., in any) automated processing of their data.

The Greek Law organizes also a procedure in case that the Data Controller does not comply with his obligations to respond to access requests: A controller has to respond to a request for access within 15 days. If the controller refuses access, he must inform not only the data subject, but also the Data Protection Authority of this refusal, and he must advise the data subject of the latter's right to appeal to the Authority (Art. 12(4)).

The sole exemption laid down in Law concerns the denial of access if the processing "is carried out on national security grounds or for the detection of particularly serious crimes." (Art. 12(4)). However, in that case the President of the Authority or his or her substitute must carry out "all necessary acts" (read: all acts needed to give as much effect to the data subject's rights and interests as possible); and in this, they must be given free access to the secret files (idem).

Correction

The *right to obtain rectification***,** *erasure or blocking* of incorrect or unlawfully processed data is, in the Law, *included* in the *right to object* to processing, although these matters are treated separately in the Directive (see Arts. 12(b) and 14(a) of the Directive). Art. 13(1) of the Law entitles the data subject to object at any time to the processing of data relating to him. Such objections shall be addressed in writing to the Controller and must contain a request for a specific action, such as correction, temporary non-use, locking, non-transfer or

[55] See Art. 12(a), first indent of the Directive.

[56] According to ….this provision goes somewhat beyond the requirements of the Directive, which requires controllers to provide data subjects only with information on *sources* to the extent that that information is "*available*" (Art. 12(a), second indent, of the Directive).

deletion. Attention must be paid to the right to object, which is not dependent upon the justification of "compelling legitimate grounds relating to his particular situation".
In this case too, the Law lays down a procedure to enable the exercise of this right. The controller must again reply to such objections within 15 days, and *in writing*. The controller must *inform* the data subject of the ***action*** taken in response to the request or, alternatively, of the *reasons* for *not complying* with the request (Art. 13(1)). If a controller has *amended* or *deleted* any data as a result of a request from a data subject, he must provide the data subject with a *copy* of the amended record (Art. 12(3)). However, the Law *does not contain the requirement included* in the Directive, that the controller must also *inform any third parties to whom the data have been disclosed* of such rectifications or deletions[57].

The Law does however again stipulate that in any case in which a controller fails to comply with a request from a data subject for correction or erasure etc., the controller must *inform the Data Protection Authority* of this refusal (see again Art. 12(3)). A right to appeal to the supervisory authority is granted where the controller does not respond to the petition or his/her reply is not satisfactory.

Notification of disclosure

The Law requires that, if the data are *disclosed* to any *third party*, the data subject must also *always* be informed of this, *before the actual disclosure* (Art. 11(3)). It must be noted that the Authority has imposed several sanctions for non compliance with this requirement.

Right to object to direct marketing

In accordance with the Directive, the Law grants data subjects an *absolute right to object to direct marketing use of their data*. Under the Law, this right is exercised by the data subject making a "*statement*" to that effect *to the Data Protection Authority* (Art. 13(3)).[58] The Data Protection Authority maintains *a list of persons who have registered their objection*, and any controller who wishes to carry out direct marketing must "*consult*" this register and *delete* from their files the persons listed in the register. The Decision 50/2000 relating to the collection of data for marketing purposes stipulates that the agent collecting the data (i.e. the person or agency actually arranging the mailing or other marketing communication) has the obligation to consult the special register (of those who do not wish to have their data processed for the purposes of direct marketing or sales promotion).

In is noteworthy that in Greece, this register is maintained by the national Data Protection Authority (rather than by industry itself, as is the case in most other countries).

[57] See Art. 12(c) of the Directive, which however requires this, provided the informing does not prove impossible or involve a disproportionate effort.
[58] The Law refers to objections to "*processing in order to promote the sale of goods or long distance services,*" but this must be read as a reference to ***direct marketing*** of goods and services.

10. Individual Remedies

The Law *grants data subjects the right to appeal to the Data Protection Authority*, if they are denied (or not given) *confirmation* as to whether data are processed on them, or *access* to their data, or if a controller refuses to comply with a request for *correction or erasure* (see Arts. 12(4) and 13(2) of the Law). The Authority has then to investigate the matter.

Data subjects can also, under the general law, apply to a *court* to obtain redress, including, where appropriate, *injunctions***,** against any processing that in any way infringes the Law, if they suffer (material or immaterial) *damage* as a result of such unlawful processing. According to the provision regulating civil liability with regard to data processing, any natural person or legal entity of private law, who in breach of this law, causes material damage shall be liable for damages in full. If the same causes non pecuniary damage, s/he shall be liable for compensation. The liability also exists when the person ought to have recognised the possibility that damage might be caused to another person. The latter provision has raised serious interpretation issues. According to the wording, the liability should be considered as objective or strict: the law imposes liability to compensate on the person who caused the prejudice regardless of his fault or other subjective factors.[59] The State may also bear civil liability for acts and omissions of its organs, under the general provisions of Introductory Law of Civil Code (Art. 105-106).

11. Supervision, Notification and Enforcement

Supervision over compliance with the Law is placed in the hands of the Data Protection Authority (Art. 15(1)). The Greek law established a supervisory authority, which started its operation on November 10th, 1997. The Greek Authority comprises a chairman, and six members[60]. The Authority has to be composed of a judge of a rank corresponding at least to that of a Counsellor of State as President and six members as follows: a) a University professor, full or associate, specialised in law, b) a University professor, full or associate, specialised in information technology, c) a University professor, full or associate, d) three persons of high standing and experience in the field of the protection of personal data. The judge-President and the professors-members may be on active service or not. The President and the members are appointed for a term of four years and nobody may serve more than eight years.

The supervisory authority constituted, already from its establishment, an "independent public authority", which per definition does not belong to the classic scheme of the separation of powers[61] and was/is not subject to the supervision by a Minister[62]. For constitutional and

[59] M. Stathopoulos, The use of personal data and the conflict between the freedoms of data controllers and the freedoms of data subjects (in Greek), Nomiko Vima (48) 2000, p. 17.

[60] See Art. 16 § 1 of the Law 2472/97

[61] There is a theoretical debate on the question if these independent agencies are - as part of a system of checks and balances – "institutional check on the majority" or "guarantor of the democratic rule of law". See P. Eleftheriadis, Constitutional Reform and the Rule of Law in Greece, West European Politics, 28:2, p. 323, E. Venizelos, The Amendment's Achievement (in Greek), Athens 2001, p. 135, 227

[62] As it concerns the material conditions of independence, the Greek legislation has granted organisational, accounting, management and functional autonomy to the DPA. Within the pre-determined

institutional reasons the Authority is "attached" to the Minister of Justice, but it is not subject to any administrative control and exercises its functions "with complete independence"(Art. 15). In the course of their duties the members of the Authority enjoy, like the judges, "personal and functional independence" and "they obey their conscience and the law". Although the Authority "reports to" the Minister of Justice, it is an *independent* agency and "*not* subject to any administrative control" (Art. 15(2)). This independence of the Authority is since 2001 guaranteed by the Constitution: according to the new Article 101A[63] the members of the supervisory authority enjoy "personal and functional independence". The President and the Members of the DPA should be appointed by the abovementioned all-party parliamentary Committee (Conference of Presidents)[64] requiring unanimity or at least four-fifths majority. In other words, these appointments should be the result of consensus between at least the two major parties[65].

The Authority has a wide range of functions, set out in a long list of paragraphs in Art. 19. Special reference should also be made to the very broad regulatory powers possessed by the Authority: it issues *opinions, recommendations, directives* and *regulations* (as referred to from time to time in this report), as well as *general instructions* for the purpose of a uniform application of the Law, and more *specific instructions* to particular *controllers*. Finally, the Data Protection Authority is to be heard before the adoption of any regulation relating to the processing and protection of personal data. The Authority has a close "institutional relationship" to the Parliament: it has to keep the Parliament informed about the violations of the law. Additionally, the DPA submits to the President of the Parliament and to the Prime Minister an annual report, which can include legislative measures proposed by the Authority. However, in most cases the annual report failed to be debated, whether by the General Assembly or by the competent Committee.

The Authority is responsible for *notification*. In that respect, controllers must notify the establishment/operation of a file andor the commencement of data processing (Art 6). Subject to the prior control and approvement/permission of the Authority are a) the processing of "sensitive personal data"[66], b) the interconnection of files containing personal data or unique personal identifiers, c) the transborder flow to third countries and d) the exemptions from exercising the individual's rights for reasons of national security or for the detection of

---

budget, the law allows the DPA to implement autonomous organisational mechanisms, for instance, as regards recruitment of staff, contracts, and administrative proceedings.

[63] Such independence is guaranteed by the Constitution for five agencies: the Data Protection Authority, the Confidentiality of Communications Authority, the National Council for Radio and Television, the Civil Service Appointments Authority and the Office of the Citizen's Advocate.

[64] The Conference of the Presidents is a collective institution of the Parliament. This institution, which was introduced by the Standing Orders of 1987, found its constitutional consolidation in the constitutional amendment of 2001. The Conference is composed by the Speaker and the Vice-Speakers of the Parliament, former Speakers of the Parliament if elected in office, the Presidents of the Standing Committees, the President of the Special Standing Committee on Institutions and Transparency, the Presidents of the Parliamentary Committees and a representative of independent MP's (provided that there are at least five of them). Following the constitutional revision of 2001, the Conference of the Presidents has assumed the responsibility to choose, unanimously or by a majority of 4/5 of its members, the members of the Independent Administrative Agencies provided for by the Constitution.

[65] In the case of the Data Protection Authority, only once the Parliament has followed this appointment procedure, i.e. by the last appointment after the resignation of the President and five members of the Data Protection Authority in November 2007. The new synthesis has been appointed 6 months after but it is not sure that this delay can be explained through a difficulty to reach a consensus.

[66] With the exemption of the cases laid down in Art. 7 A of the Law 2472/97

particularly serious crimes. In connection with the notification requirements, the Authority is charged with maintaining a number of *registers*[67]. Access to the first five of the above files is *open to the public*, but access to the *secret files register* is generally not allowed (although the Authority can allow access if appropriate) (Art. 19(5)).

The Authority can carry out "*administrative examinations*" and more specific *investigations* into suspected or alleged unlawful processing. either on the basis of a *complaint from a data subject*, or *ex officio* (Art. 19(1)(g) and (h)). Almost from the outset, the Greek DPA has conducted audits either "ex officio" or in the context of a priori control or a complaint, in order to grant a permit for a file/processing. In this respect, the Authority is granted *very wide powers*: subject only to a limited exception with regard to national security files[68], the Authority has the right to demand access to any personal data and the right to collect any kind of other information for the purposes of such review, notwithstanding any kind of confidentiality (Art. 19(1)(h)). In order to exercise these rights of access to such data the Authority can also enter—it would appear, without warrant—any premises on which such data (or the automated or manual files, in which the data are held) can be found.[69] All public authorities are obliged to *render assistance* to the Data Protection Authority (Art. 19(10)). The Authority can also exercise these powers on behalf of a *foreign data protection authority* (Art. 19(1)(n)).

The Greek DPA also has the overall competence for the enforcement/application of Law 3471/06 concerning the protection of personal data in the electronic communications sector (Art. 13§1 of Law 3471/06). However, some of the competences provided in the abovementioned law have been entrusted to the "Hellenic Authority for the Information and Communication Security and Privacy": a) the competence regarding the exceptional processing of location data in emergency cases (Art. 6§4 of Law 3471/06) and b) the competence regarding the calling line identification in cases of malicious or emergency calls (Art. 8§7 of Law 3471/06). The legislator has considered that these competences pertain to the general competence of this Authority.

Equally important is its role as "Data Protection Ombudsman" for individuals[70] The DPA considerscomplaints and reports lodged by data subjects, having a wide-ranging discretion in deciding on such complaints. The Authority has the power to impose what is called an "*administrative fine,*" i.e., a fine that must be paid if a court upholds the view of the Authority that the processing in question was unlawful (or if the controller concerned accepts

[67] Concretely: a)*files and processing register* (which contains the notified particulars of all processing notified to the Authority), b) *permits register* (which contains the permits issued by the Authority for the establishment and operation of files containing sensitive data etc.), c) *interconnections register* (which contains the declarations and permits issued by the Authority for the interconnection of files), d) *register of persons who do not want to be receive direct marketing messages*;*transfer permits register* (which contains the permits for the transfer of personal data, as further discussed below, at 10) and e) *secret files register*, which contains information on "files kept by the Ministry of National Defence, the Ministry of Public Order and the National Intelligence Service for reasons of national security or for the detection of particularly serious crimes" and on interconnections with these files.

[68] These files may be accessed and controlled by the President of the Authority or by a Member specifically designated by the President.

[69] If the Authority is investigating a possible criminal offence under the Act, its staff has police powers: Art. 22(10).

[70] On its website the DPA describes as its "primary goal" the "protection of citizens from the unlawful processing of their personal data and their assistance in case it is established that their rights have been violated in any sector (financial, health, insurance, education, public administration, transport, mass media etc.)".

this without a fight) (Art. 19(1)(f)). In urgent cases, the President can order the *immediate suspension* of a particular processing operation (Art. 19(7*a*)). The Authority may also impose fines on the State, i.e. Ministries, State authorities/agencies, local authorities. Such fines have been for example imposed on the Ministry of Public Order for non-compliance with the DPA's Decision concerning the lawful use of CCTV in public places or on the Ministry of Justice for non-compliance with the data security requirements for archives containing sensitive data of juvenile delinquents[71]. The Authority places emphasis on the symbolic value of such a sanction[72] imposing relatively low fines.

12. Sectoral (Self-) Regulation and Codes of Conduct

Concerning codes of conduct and other self-regulatory instruments, there is no specific article included in the Law. However, the Greek legislation provides for the possibility of adoption of codes of conduct. This possibility is laid down as an Authority's competence, which invites and assists professional societies and similar associations towards the establishment of codes of conduct to guarantee the effective protection of privacy and the rights and freedoms of persons in their field of activity(Art. 19(1)(b)).

In any case, self-regulation has not a tradition and is regarded as an auxiliary means to implement and supplement legislation in the specific contexts of data processing and consequently, codes of conduct can only operate within the prefixed legal framework. The DPA has not initiated till now self-regulatory actions. Noteworthy is the initiative of the Authority to work in cooperation with the European Network Information Security Agency (ENISA) on guidelines in order to fight unsolicited electronic communication (spam)[73].

- o – O – o -

[71] The DPA has imposed fines raising to the amount of 5.000 Euros to the Ministry of Public Order and 5.000 Euros (Decision 7/2008) to the Ministry of Justice. However, the DPA has imposed on a Minister a fine in height of 10.000 for revealing through publication at the Government's Official Gazette of an official's health data. See Annual Report 2003, p. 36. In another case the DPA has imposed on a Minister a fine of 20.000 for non-compliance with the ruling of the Authority concerning the right of access of an official to his record.

[72] Fines are effected pursuant to the provisions of the Public Revenues Collection Code. They are revenues of the State and not of the Data Protection Authority. One of the factors possibly helpful as regards the independence of the Authority is related to the intended use of the financial resources via those fines – which are not paid directly to the DPA, although it is provided that a portion of the fines could be paid back to the DPA.

[73] For more details see Annual Report for the year 2007 p. 81