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

Greece

Elaborated by Ass. Prof. Dr. Lilian Mitrou
University of the Aegean

February 2008

CONTENTS 2

EXECUTIVE SUMMARY 3

EXECUTIVE SUMMARY

Overview

[1]. The Hellenic Constitution (1975/1986/2001) recognizes explicitly the right of privacy (Art. 9), the right to protection of personal data (Art. 9 A) as well as the freedom of communications (Art. 19). Law 2472/97 transposed the Data Protection Directive into greek law. The Greek legislator opted for a general legal framework, which is applicable to both the private and the public sector and covers automated processing but also that carried out by conventional means. Law 2472/97 is complemented by Law 3471/06, which contains provisions relating to the protection of privacy and data protection in the electronic communications sector.

Data Protection Authority

[2]. The Greek law established an "independent public authority" in charge of the monitoring of the enforcement of the law. Since 2001, the supervisory authority and its independence are guaranteed by the Constitution (Art. 9A in combination with Art. 101A). The appointment by a parliamentary committee (with unanimity or at-least four-fifths majority) aims at strengthening its independence and democratic legitimacy. The Greek legislation has granted organisational, accounting, management and functional autonomy to the Data Protection Authority (DPA). The Greek law introduced a system of control, which, in essence, makes the Authority the decisive factor on which the implementation of the legislative provisions pivots. The DPA is endowed with extensive and significant powers and tasks (investigative, regulatory, advisory powers and powers of – binding -decision and intervention). In its early years the Authority had consciously concentrated on its regulatory activities as well as on auditing activities. The Data Protection Authority gives constantly specific advice to data controllers in the private and – also and mainly – in the public sector. In the last years it seems to be less proactive, as its activity is dominated by the handling of individual complaints.

Compliance

[3]. Actually there is no incontestable evidence available indicating compliance or lack of compliance with the law. Compliance with notification/prior notification duties can be assessed neither on the basis of statistics nor on the basis of other evidence. During the last years the decreasing number of notifications is explained as a result of the notification flood of the early years and the wide exemptions from notification requirements adopted in 2000. As far as compliance with the decisions of the DPA is concerned, the controllers comply mostly with the decisions of the Authority or with these of Council of State (Highest Administrative Court), which in the vast majority of cases upheld the rulings of the DPA.

Sanctions, Compensations and Legal Consequences

[4]. Greece has adopted administrative sanctions to be imposed by the DPA as well as an impressive array of penal sanctions in case of infringements of the law. Greek Data Protection legislation provides for judicial remedies and civil liability in case where a person has suffered (pecuniary and non-pecuniary/moral) damage as a result of unlawful processing. The Authority has till now refrained itself from imposing very often the (highest) sanctions allowed by the law. The Courts have shown caution in relation to penal sanctions but they have relatively often ruled a restitution of the moral damage caused to the individual.

Rights awareness

[5]. There are no specific studies/surveys on awareness regarding data protection duties and rights. The DPA is playing an important role as educator in order to raise awareness among data controllers, especially in the public sector. The DPA has focused its efforts for informing the public through its presence on the web. The increasing number of data subjects' complaints and petitions is regarded as result of subject's self-consciousness and a growing awareness among the public on data protection issues.

Analysis of Deficiencies

[6]. From a fundamental rights perspective, a main deficiency of the regulatory framework consists exactly in the exemption from the scope of application of the Law and the monitoring through the Data Protection Authority of the processing of personal data by the police and in general the security authorities, which has been introduced by Art. 8 of Law 3625/07. This legislative measure raises significant concerns in relation to its compliance with a) the Constitution, which recognises explicitly the right to data protection and the control competence of the independent authority and b) other international legally binding instruments (ECHR, Additional Protocol of Convention 108, Schengen Convention/Europol Convention etc.)

[7]. A second major problem concerns the transparency and consistency of the legal framework concerning data protection in the electronic communications sector. The existence of more laws that are simultaneously applicable and the overlapping competences of the DPA and the Hellenic Authority for the Information and Communication Security and Privacy raise a lot of problems concerning the effective and consistent application of the respective rules.

[8]. The powerful statutory means possessed by the independent authority does not in itself guarantee the effectiveness of data protection. The activity of the DPA is dominated by individual cases/complaints at the expense of other matters and mainly the proactive audit and the regulatory activities of the DPA. Apart from the necessary regulatory/organisational measures the DPA should consider how to fulfil its constitutional/institutional duties while avoiding its decline into bureaucracy and how to combine in a balanced and effective way the role of an informational Ombudsman with that of a political institution for control and dialogue with the state and the citizens on the developments in technology and its applications, and their effects on freedoms and on the organisation of state, society and economy.

Good Practice

[9]. Data protection is a relatively new legislative material, which has not yet been integrated in the practice of public and private organisations. In addition, the data protection system has been structured in such a way that the Authority is pivotal for the interpretation and enforcement of the relevant provisions. The result is that the absence

of measures and practices deriving from other organizations and public bodies.

1. Overview

[10]. 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, states 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".

[11]. The constitutional revision of 2001 added a new provision granting individuals an explicit right to protection of their personal information. According to Article 9A, "all persons have the right to be protected from the collection, processing and use, especially by electronic means, of their personal data, as specified by law". The existence of an independent data protection authority has also developed into a constitutional element of the right to data protection: 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." Before the introduction of this new provision, the legal doctrine as well as the jurisprudence regarded art 9 (protection of private life), art 2§1 (dignity of the person) and art 5§1 (right to free development of personality and participation in the political, social and economic life) as the basis for the recognition of a "right to informational self-determination".

[12]. Article 19 of the Constitution protects communicational privacy. It states that "secrecy of letters 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. Article 19§2 now states that matters relating to the establishment, operation and powers of the independent authority ensuring the secrecy of communications shall be specified by law. As additional garantuee 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.

[13]. Greece has signed and ratified the European Convention for the Protection of Human Rights and Fundamental Freedoms. 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. 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 data protection legislation in place, i.e. contrary to the respective requirement of the Convention.

[14]. Although an expert commission submitted the first draft law in 1983, the Greek Data Protection Law was approved fourteen years later, in April 1997. In the meantime, draft-laws were introduced to Parliament twice by the Socialist Party (once as a draft law proposed by the Government and once as a law proposal by the opposition) and once by the Conservative Party; however, due to the reactions/resistance of certain parts of the Public Administration (national and public security agencies) as well as of certain organisations and social groups (church organisations, left-wing NGOs) these legislative attempts have proved fruitless. The pressure on Greece became stronger after the enactment of the EU Data Protection Directive 95/46/EC and the need to meet the requirements in order to join the Schengen Agreement.[1] Due also to the absence of the need to amend existing legislation, Greece has succeeded in implementing the Directive well ahead of the determined schedule (October 1998). The Greek Data Protection Law (Law 2472/97 "on the Protection of Individuals with regard to the processing of personal data") has been approved by the Hellenic Parliament on 26.03.97 and published in the Official Gazette on 10.03.1997. The provisions came substantially into force after the appointment of the Data Protection Authority on 10.11.1997.

[15]. By means of the Law 2472/97 the legislator transposed the Data Protection Directive into national law and delineated the constitutionally acceptable processing of personal data. The similarities between the approach taken by the Greek legislator and that of the European Union are obvious and at the same time reasonable, as the Hellenic Parliament was expected to adapt the

[1] The Schengen Convention requires that data protection safeguards should exist in each Contracting Party. These safeguards include supervision by a national independent supervisory authority, which should be designated by each Contracting Party and have central responsibility for the national section of the Schengen Information System (Art. 108).

regulations to the standards and binding demands laid down by the Directive. The law does not follow exactly the same structure but all of the main provisions of the directive can be found. The Greek legislator has made full use of the discretion he had from the Directive in order to enhance further the protection of citizens: the law did not introduce the exemptions of Art. 13 of the Directive. Furthermore, the law adopted a wider list of sensitive data (in relation to that mentioned by the Directive in Art. 8 as "special categories of data") or a wider definition of the "file".

[16]. The provisions of the law cover, without exceptions and without differentiations, automated processing but also processing carried out by conventional means. Law 2472/98 constitutes a framework of rules, which rest on four pillars: a) a system of substantive regulations[2], 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.

[17]. The Greek data protection law places particular emphasis on the "consent" of the data subject to the processing of his/her personal data. 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[3].

[18]. A main characteristic of the Greek data protection law is the classification of personal data based on its perceived sensitivity. The Act distinguishes between personal data and sensitive personal data[4], which are subject to strict(er) safeguards and procedural formalities[5]. The Greek legislator has also considered that the so-called

[2] 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.

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

[4] The law defines as sensitive personal data 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 (Art. 2 b).

[5] The creation of the file containing "simple" personal data and the respective processing of the said data is subject to notification to the Data Protection Authority whereas the creation of the file containing sensitive data and the respective processing is subject to the prior control of the Authority, which grants a permit.

"interconnection of files"[6] is likely to present specific risks[7]: the interconnection of files is – under the conditions laid down in law- subject to notification or prior checking by the supervisory authority[8].

[19]. Since the adoption of the law, there have been several amendments. A first major amendment was enacted through the Law 2819/2000, which added Art. 7a allowing wide exemptions[9] from the obligation to notify the Data Protection Authority and receive a permit. 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 "file"[10] 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. The last 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 by judicial authorities, prosecutors and security/police authorities for the purposes of law enforcement from the application of the law, 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).

[20]. Law 2472/97 has been complemented by Law 2774/99 on the Protection of Personal Data in Telecommunications Sector[11]. Law 2774/99 has been amended by the Law 3471/06 in order to harmonize the respective Greek legislation with the Directive 2002/58/EC. The Law 3471/06 contains provisions relating to the secrecy of electronic

6 According to Art. 2 f of the Law 2472/97 term "Interconnection" refers to a form of processing consisting in the possibility of co-relating the data from a file to the data from a file or files kept by another Controller or Controllers or with data from a file or files kept by the same Controller for another purpose.

7 See Art. 20 as well as Recitals 53 and 54 of the Directive 95/46/EC

8 According to Art. 8 § 3 of the Law 2472/97, the interconnection of files is subject to prior notification and permit to be issued by the DPA, if at least one of the files about to be interconnected contains sensitive data or if the interconnection results to the disclosure of sensitive data or if for the implementation of the interconnection a unique identifier is to be used.

9 Exempted from notification/prior notification requirements is the processing concerning personnel files, customer files and membership of societies, associations, and political parties. Exempted is also the processing carried out by doctors or other persons rendering medical services, attorneys-barristers and notaries, as well as judicial authorities.

10 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 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.

11 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.

communications services, the processing of traffic data, the itemized billings, the identification of calling-connected line, the directories of subscribers and the unsolicited calls. It is noteworthy that the 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"[12] and d) possibility of anonymous use and payment of electronic communication services.

[21]. 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[13], b) the re-use of public sector information[14] or c) the processing of data for the prevention and detection of organised crime[15]. 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.

[22]. Actually, there is no national debate (in the meaning of public discussion/discourse) in terms of deficiencies. The major opposition Party (Panhellenic Socialist Party) has proposed (2007) the unification of the Data Protection Authority and the Hellenic Authority for the Information and Communication Security and Privacy (see Par 45 of the Assessemt Report) in order to rationalize the application of the respective laws.

[12] 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.

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

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

[15] 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.

2. Data Protection Authority

[23]. The starting point of the Greek legislator was that efficient legislation presupposes the establishment of a system of «external supervision» in the form of an independent authority, in order to ensure a good level of compliance with the law, to provide support and help to individuals and to monitor existing regulations. The Greek law established a supervisory authority, which started its operation on November 10th, 1997.

[24]. A constituent part of the very concept of control is the independence of the organ of control, understood as the total of statutory and functional conditions, which make possible the pursuit of the special objectives of control and their achievement. The Greek legislator has initially founded the independence of the Data Protection Authority on the following axes: a) the selection of the statutory form of the "independent administrative authority", in one of the more genuine versions of this model, b) the involvement of the Parliament in the selection of the members of the Authority. Initially, i.e. before the constitutional amendment of 2001, the President of the Authority was appointed by the Cabinet whether the six other members were selected by the simple majority of an all-party parliamentary committee (the so-called "Conference of Presidents"). However, the purpose of the Parliament's involvement was to ensure the transparency and the democratic review of policy in relation to the protection of personal data. It should also accentuate the legitimacy of the Authority and strengthen its position and independence vis- a -vis the Executive.

[25]. 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[16] and was/is not subject to the supervision by a Minister. For constitutional and 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".

[16] 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

[26]. This independence of the Authority is since 2001 guaranteed by the Constitution: according to the new Article 101A[17] 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)[18] 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[19].

[27]. This parliamentary appointment enhances without doubt the democratic legitimisation of the Authority. This is particularly important in view of the fact that the decisions and acts of this - independent but administrative- authority are not subject to typical parliamentary scrutiny[20]. It is uncertain what role these provisions will eventually play in securing the true independence[21], as independence must not merely be safeguarded but, at the end, must be validated and realised through the effectiveness[22] of the Authority and the data protection system as a whole.

[28]. The Greek Authority comprises a chairman, and six members[23], elected by the so –called "Conference of Presidents". The Authority

17 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.

18 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.

19 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.

20 However the Parlamentarian Committee for Institutions and Transparency (Επιτροπή Θεσμών και Διαφάνειας), which "supervises the Independent Authorities" (Art. 43 A § 2 of the Standing Order of the Parliament) may invite the President and the Members of the Authority to inform the Parliament and give explanations about the issues falling under their competence.

21 P. Eleftheriadis (2005), Constitutional Reform and the Rule of Law in Greece, West European Politics, 28:2, p. 324

22 See L. Mitrou, The Greek Law on the Protection of Personal Data, in L. Sicilianos-M. Gavouneli (eds.), Scientific and Technological Developments and Human Rights, Athens 2001, p. 151.

23 See Art. 16 § 1 of the Law 2472/97

has to be composed of a judge of a rank corresponding at least to that of a Counsellor of State (Conseiller d'État, Σύμβουλος Επικρατείας) 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.

[29]. The Authority has its own budget[24] and is assisted by its own Secretariat[25]. The Secretariat operates at the directorate level and is structured in three departments: a) Auditors' Department, b) Public Realtions and Communications Department, c) Department of Administration and Budgetary Affairs. Each of the departments has a supervisor. All departments are supervised by the Director of the Secretariat. It is worth noting that in the case of the Greek DPA it is not exactly the "legal image"[26], which seems to dominate the data protection approach. Even if the majority of the Committee consists of lawyers, the Authority from its establishment till now is hiring consciously lawyers and computer scientists in a fully balanced proportion.

[30]. The Greek legislation has granted organisational, accounting, management and functional autonomy to DPA. Within the pre-determined budget, the law allows the DPA to implement autonomous organisational mechanisms, for instance, as regards recruitment of staff, contracts, and administrative proceedings. The resources allocated to the DPA are not negligible but they are considered to be insufficient given the scope of the application of the law and the tasks performed by the DPA. According to the DPA due to the restricted resources it has not the possibility to expand the scope of preventive and controlling actions/activities and to launch wide-ranging awareness actions..

[31]. As far as it concerns the remit of the DPA, the Authority's task is the supervision of the data protection law and of other provisions pertaining to the protection of individuals with respect to the

[24] According to Art. 15 § 3 the budget of the Authority is entered in a special "section" which is integrated on the annual budget of the Ministry of Justice. The President of the Authority or his substitute is the authorizing Officer for the expenditure.

[25] See Annex I

[26] See about P. Hustinx (EDPS), "Perspectives of Independent Authorities: independence and more effectiveness", Proceedings of the Conference "The Independent Authorities in Modern Democracy", April 2007.

processing of personal data. The Data Protection Authority is endowed with extensive and significant powers and tasks (investigative powers and powers of decision and intervention). It has a wide range of functions, set out in a long list of paragraphs in Art. 19: it issues opinions, recommendations, directives and regulations, as well as general instructions for the purpose of a uniform application of the Law, and more specific instructions to particular controllers. It encourages and assists associations, etc. in the drafting of codes of conduct. In the event that, the President may, upon request of the party concerned, issue a provisional order for immediate suspension of the processing or the file operation, in whole or in part.

[32]. Ex officio or pursuant to a complaint or a reported infringement, the Data Protection Authority can conduct investigations and administrative inspections of any file. In cases that the protection of an individual with regard to the processing of personal data calls for immediate decision-making the DPA may take provisional measures such as the suspension of the processing. The DPA has a right of access and the right to collect information, obligations to secrecy notwithstanding. Exceptionally, the Authority shall not have access to identity data relating to associates and contained in files kept for reasons of national security or for the detection of particularly serious crimes.

[33]. The Authority can indicate infringements to the judicial authorities and but it can also impose administrative sanctions. The Authority is responsible for notification and prior notification according to the procedures provided in Law. In connection with this, the Authority is charged with maintaining a number of registers.

[34]. A limitation of the remit of the DPA consists exactly in 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.

[35]. The Greek law introduced a system of control, which, in essence, makes the Authority the decisive factor on which the implementation of the legislative provisions pivots. This is the model of control in which the control organ, apart from the stricto sensu monitoring of compliance with the regulations, has a lot of tasks, is endowed with broad decision-making powers and is equipped with the means, which allow it to impose its decisions and views, always subject to judicial review. Remedies against the binding decisions of the Authority may be filed by the natural or legal persons affected by the decisions of the DPA and also by the State. Such remedy shall be initiated by the competent Minister as the case may.

[36]. Subject to the prior control and approvement/permission of the Authority are a) the processing of "sensitive personal data"[27], 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 particularly serious crimes. The main characteristic of the system of preventive control does not lie in the chronological transposition of the moment of legality control but in the transference of the decision outside the data controller and the Executive.

[37]. The Authority's task is in general described as "the supervision of the data protection law and of other provisions pertaining to the protection of individuals with respect to the processing of personal data" (Art. 15 § 1). Ex officio or pursuant to a complaint or a reported infringement, the Data Protection Authority can conduct investigations and administrative inspections of any file. For this purpose it has a right of access and the right to collect information, obligations to secrecy notwithstanding. It must give recommendations and instructions to data controllers and issue regulations on the detailed application of the law. It encourages and assists the preparation of codes of practice. The Authority can indicate infringements to the judicial authorities and but it can also impose administrative sanctions.

[38]. Special reference should also be made to the very broad regulatory powers possessed by the Authority: issuing of instructions with the purpose of ensuring uniform implementation of the regulations, issuing of regulations pertaining to special, technical and detailed matters, issuing of specific rules for processing for the most common categories of data/files. Finally, the Data Protection Authority is to be heard before the adoption of any regulation relating to the processing and protection of personal data.

[39]. Especially during the first phase, the DPA has set as priority the clarification of the applicable rules and has focused on its quasi-regulatory competences. The DPA has issued a number of so-called "instructions" (Directives –Οδηγίες) for the purpose of a uniform application of the rules pertaining to the protection of data subjects. The Authority issued "Directives"[28] (relating to processing with regard to direct marketing/advertising and the ascertainment of

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

[28] Law 2472/97 refers to "instructions for the purpose of a uniform application of the rules pertaining to the protection of individuals against the processing of personal data " (Art. 19 § 1 a) but the Authority uses the term "Directives".

credibility (50/2000), Closed Circuit Television systems (2000)[29] or DNA testing for law enforcement purposes (2001). The DPA has also issued a Directive containing guidelines covering data protection in the workplace in particular surveillance of phone calls and e-mails (115/2001). To the extent that it is also competent for compliance with the data security requirements of the respective law, it issues instructions also concerning the security of information systems.

[40]. 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.

[41]. Equally important is its role as "Data Protection Ombudsman" for individuals, when the latter face difficulties in relation to the processing of their data and/or in the exercise of rights granted to them by the law.[30] The DPA is entrusted with the task of considering complaints and reports lodged by data subjects and it has wide-ranging discretion in deciding on such complaints. This does not mean that the DPA should be regarded as a special court. However, it carries out quasi-judicial activity especially in respect to its auditing power, the possibility of hearing both "parties", the enforceability of its decisions, its provision to be challenged before ordinary courts.

[42]. The Data Protection Authority guarantees the transparency of data processing and therefore it maintains six registers: the Register of Files and Data Processing Activities, the Register of Permits for holding sensitive data, the Register of Interconnections, the Register of persons who do not wish to receive mailings, the Register of Transfer Permits and the Register of Confidential Files, which contains files maintained by the Ministry of National Defence, the Ministry of Public Order[31] and the National Information Agency for reasons of national security or for the investigation of especially serious crimes. As far as it concerns transparency of its own action

[29] In September 2000, the DPA set out guidelines concerning the recording, use, monitoring, and retention of personal information through the use of CCTV and set strict criteria for the lawfulness of these applocations.

[30] 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.)".

[31] The former Ministry of Public Order forms now an internal part of the Ministry of Interior and Public Administration.

and accessibility of its own action, the DPA is making its opinions and decisions readily available via its website (www.dpa.gr).

[43]. 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.

[44]. 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. Audits vary in terms of frequency and rigour. In Greece audits are a constant, however sometimes under-resourced, component of the DPA's agenda.

[45]. Especially in the early years, the Authority had consciously concentrated its auditing activities in specific sectors[32]. Additionally, it is not clear if the Authority has developed a specific methodology for the examination of all phases of data processing within a controlled organisation, which is - to a large extent - due to the abundance of its competences and the amplitude/diversity of the controlled sectors/organisations.

[46]. The Data Protection Authority gives constantly advice to data controllers in the private and – also and mainly – in the public sector. This consultative support takes mainly the form of responding to specific, ad hoc questions relating to specific issues. The DPA is expecting to be consulted when new systems, which have privacy implications, are being developed. Many information systems and data bases have been developed in the public sector during the last years without the DPA having the possibility to propose built-in privacy protection elements at the outset of the design of such systems. A recent case concerns the Decisions Database of the Supreme Administrative Court (Council of State, Συμβούλιο της Επικρατείας): in this case the DPA has insisted on the anonymisation of the archived

[32] For example in 1999 the Authority set as priority the auditing of the security sector as well as the bank sector (with focus on the so-called blacklist database "Teiresias"), in 2000 the public administration and health sector, in 2001 the health and the assurance sector, in 2002 the health sector, Internet service providers and IT-system companies.

decisions while the Council of State has already spent the financial resources devoted to the project by designing a database with decisions containing the names of the parties.

[47]. In case the Authority is consulted[33], this tends to occur outside the public scrutiny and therefore the influence of the Authority cannot be measured. The DPA had until now only in very few cases the opportunity of giving testimony on data protection issues at hearings of the Parliament. The Authority has acted as a policy adviser, either by proposing amendments of the law or by commenting on privacy implications of proposed legislation. It is worthy to note that in the vast majority of cases it was the Data Protection Authority, which has proposed the amendments to the data protection legislation. That was the case concerning the amendments adopted with Laws 2819/00 and 3471/06 However, the last amendment of the Law 2472/97 through the Law 3625/2007, which has restricted the scope of the application of the law and the respective competences of the DPA, took place not only without the involvement of the DPA but also contrary to the decisions of the Authority. The Authority was/is also consulted either by participating in draft-law committees[34] or by giving its opinion[35].

[48]. As a rule, the DPA regards as legal basis for exercising its competences not only the national law (Art. 9 and 9A of the Constitution and the Laws 2472/97 and/or 3471/06). Article 8 of the European Treaty on Human Rights for the protection of private life, the Convention 108/1981 of the Council of Europe, Articles 7 (protection of private life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union and finally EU legislation (in specific Directives 95/46/EC and 2002/58/EC) are referred to and serve as legal basis when dealing with data protection issues.

[49]. By analysing the Decisions of the DPA it seems that the Authority does not consider the Opinions of the Art. 29 Data Protection Working Party as a binding legal source. The Greek DPA regards these Opinions merely as a reinforcing instrument for its argumentation especially in cases of a more regulatory character. Such reference to the Art. 29 Opinions is made for example in Opinion 115/2001 or in

[33] As in the case of a Project concerning the design of a Portal in order to offer e-government services, containing plans for use of unique identifiers and extensive data-sharing in the delivery of public services.

[34] The DPA is represented in the Committee responsible for the transposition of the Data Retention Directive.

[35] For example the DPA has given its Opinion in relation to amendments of the Consumers Protection Law or to the Establishment of the Hellenic Cadastre. See Annual Report 2005, p. 23 ff.

the Decision 1122/00, i.e. the Directive concerning the use of CCTV for safety and security purposes.

[50]. In order to understand and assess the institutional privacy protection system it is important to take into consideration the provisions relating to the communications secrecy and especially those related to the supervisory aythority. After the adoption of the respective constitututional amendment, the Law 3115/2003 established the Hellenic Authority for the Information and Communication Security and Privacy[36] in order to protect the secrecy of mailing, free correspondence or communication in any possible way as well as the security of networks and information. This Authority is in charge of monitoring the compliace with the provisions regarding the lawful interception of communications (Law 2225/94 in combination with Law 3115/03). In addition, the Hellenic Authority for the Information and Communication Security and Privacy has the competence of auditing - ex officio or on the basis of a complaint – public authorities as well as private organisations/companies which are active in the sector of postal and communcation services. In this context, the Hellenic Authority for the Information and Communication Security and Privacy may give instructions or issue recommendations and/or legally binding regulations. This independent Authority, regarding itself as the authority in charge to deal with security issues pertaining to data, databases, IT-systems and networks, has issued regulations for securing secrecy[37].

[51]. Greece has not yet transposed the Data Retention Directive (2006/24/EC). However the draft-law prepared by the competent Committee proposes that the Hellenic Authority for the Information and Communication Security and Privacy (and not the DPA) should be designated as the Authority responsible for monitoring the application of the data retention framework[38]. As noted in other parts of the Report, from the legal point of view the awareness raising role of the DPA concerns its possibility/responsibility to inform the Parliament about breaches of the law, to inform the media about data

[36] For more information about the Law 3115/2003 and the Hellenic Authority on Information and Communication Security and Privacy (ΑΔΑΕ) see www.adae.gr

[37] A) Regulation for securing secrecy in mobile communications, b) Regulation for securing secrecy in fixed communications, c) Regulation for securing secrecy in wireless networks, d) Regulation for securing secrecy in internet communications and in relevant services and applications, e) Regulation for securing secrecy in internet infrastructure, f) Regulation for securing secrecy in applications and the use of the internet, g) Regulation for securing secrecy in mail services, Regulation for securing secrecy when using ATMs.

[38] As the general data protection framework is applicable to the data to be retained for the purposes of data retention rules (Recital 15 of Directive 2006/24/EC) Art. 9 lays down the possibility (but not the obligation) to designate the Data Protection Authority as the authority in charge of controlling the application of data retention rules.

protection issues and concerns and to issue instructions to controllers for the purpose of a uniform application of data protection rules. The DPA reports only issues of major importance to the media. It has mainly tried and is still trying to raise awareness among the data controllers - with an emphasis on the public sector - by organising seminars or participating in educational or other activities organised by the public and private sector. The main instrument for informing the public is the website of the Authority. As mentioned in the Report, since 2002, the DPA has focused its efforts for informing the public on publishing a lot of information material, including brief analysis of the legal instruments, the rules governing specific files and sectors, FAQs and the potential source of problems for data subjects. Regarding the awareness raising role of the data protection authority, please refer to Chapter 5.

3. Compliance

[52]. As described above, Law 2472/97 introduced initially a system of universal notification: all controllers were required to declare: name and address, a description of the purpose, the type of data subject to processing, the time period intended to maintain the processing operation or the filing system, the recipients of the data, the possible transfers to non-EU countries, the principal characteristics of the data security systems. The Greek legislation refrained from the possibility for exceptions and simplifications to registration and notification procedures offered by the Directive, as the legislator considered this notification requirement as a pedagogical and informational mean for the data controllers.

[53]. In the early years and till the amendment of the law introducing exemptions form notification and prior notification requirement (2000) the DPA received in 1999 77.240 notifications and in 2000 65.000 notifications, numbers that have been drastically reduced after 2001[39]. The Authority regards only a percentage of them[40] as "important from the point of view of data protection", without specifying the criteria by which some notifications are categorized as "important".

[39] Particularly in 2001 990 notifications, in 2002 238 notifications, in 2003 283 notifications, in 2004 415 notifications, in 2005 202 notifications, in 2006 251 notifications and in 2007 560 notifications have been submitted to the DPA.

[40] For example 176 out of 415 in 2004, 97 out of 202 in 2005, 143 out of 251 in 2006 and 80 out of 560 in 2007.

[54]. The drastic decrease of the notifications' numbers is – according to the Authority – due to the fact that most of the files/processing procedures have been notified at the first years of the application of the law[41] and does not indicate necessarily and per se failure to comply with the procedural requirements of the legislation. However, as data controllers are also obliged to notify any modification of the data concerning the file/processing[42] in writing and without any undue delay to the Authority, the notifications' number seems to be very low.

[55]. As far as compliance with the decisions of the DPA is concerned, in the vast majority of cases the controllers comply with the decisions of the Authority or with those of Council of State, in cases that the Supreme Administrative Court upheld the rulings of the DPA[43]. State authorities comply with the Decisions of the DPA in the vast majority of cases. Only in few cases has the State taken legal action against the DPA by asking the annulment of its Decisions by the Council of State[44]. In other cases the Government has amended the relevant laws in order to comply with the DPA's rulings[45].

[56]. A famous case of non-compliance which raised serious concerns and public outcry was the use by the Greek Police of CCTV –systems for filming political demonstrations despite the binding contrary Decisions 63/2004 and 58/2005 of the Authority regarding the use of cameras in public places[46], while the ruling of the DPA was pending before the Plenary of Council of State[47]. Additionally, the auditors of the Authority were not allowed to access the premises of the police in order to control compliance with the DPA's decisions[48]. The Chairman and most of the members of the Authority handed in their

41 See Annual Report 2001 pp. 79f.

42 Art. 6 § 4 of the Law 2472/97

43 Which is most often the case. The Council of State has upheld the vast majority of DPA's Decisions, which have been appealed. Up to the end of 2007 the Supreme Administrative Court had annuled only three of the Decisions of the DPA, the two of them for procedural faults.

44 The Ministry of Transport and Communications asked for the annulment of the DPA's decision that related to the documents required for applying for a driving licence. The Ministry of Public Order appealed against the Decisions of the DPA concerning the use of CCTV systems in public places.

45 A noteworthy example is the change of the citizens identity cards' content in order to comply with the DPA's decision (15/05/2000). Another example is the adoption of a legal provision pertaining to the processing of employees' medical data in compliance with the suggestions which the DPA has made on the ground of a complaint (Art. 8 of the Law 3144/2003).

46 For more information about the Decision 58/2005 see Annex II

47 The Greek Ministry for Public Order made an application to the Council of State seeking to overturn the Authority's decisions.

48 Contrary to Art. 19§1 h of the Law 2472/97, which grants the Authority the right of access to personal data and the right to collect any kind of information for the purposes of such review, notwithstanding any kind of confidentiality.

resignations on Monday 19 November 2007 in protestation for an infringement of their statutory terms of reference and non-compliance with their decisions[49].

[57]. The Greek legislator has not adopted the option provided by the Directive 95/46/EC, which allows the appointment of an internal privacy/data protection officer[50]. It is noteworthy that recently (July 2008) a law concerning the assurance of telecommunications secrecy (Law 3674/08) imposes on communication services and network providers the obligation to appoint an internal "secrecy officer", who should be in charge of ensuring the security of systems and networks in order to protect the secrecy of communications. The appointment of the "secrecy officer" has to be reported to the Hellenic Authority for the Information and Communication Security and Privacy[51] as well as to the Data Protection Authority, which can ask for his/her replacement.

[58]. The DPA has issued a number of regulatory acts and decisions related to the protection of personal data in the employment sector. In September 2001 the DPA issued the Directive 115/2001[52] setting up strict limits on the collection and processing of personal data. According to the Directive, the implementation of the general data protection rules, due to their horizontal nature, did not take into account the particular nature of the employment relationship, which is characterized mainly by the inherent inequality of the parties. Although this Directive is not a binding legal instrument in a strict sense but more a "soft law" instrument, the Authority affirms its interpretation and position in relation to the application of the general rules in this specific employment context.

[59]. The Directive contains general principles and quite detailed provisions concerning the collection and processing of – simple and sensitive – personal data, the rights of the individuals and their representatives, the monitoring of the workplace as well as the e-mail and internet use monitoring. Due to the inherent asymmetry of power that characterizes the employer –employee relationship, the DPA rejects consent of the individual as a ground that legitimises by itself

[49] The (former) President of the Authority D. Gourgourakis, a former senior judge, characterized the breach of the DPA's decision "a blow to the authority's independence".

[50] Some big, mostly multinational, private companies have appointed an internal data protection or compliance officer, who deals with the protection of the consumers' privacy rights or –in some cases- with the protection of employees' data.

[51] Actually, this is the English title used by the Authority for the Ensuring of Communication Secrecy (Αρχή Διασφάλισης Απορρήτου των Επικοινωνιών – ΑΔΑΕ). The title used may cause misinterpretation and confusion in relation to the competencies of the abovementioned Authority.

[52] The text of this Directive is attached as Annex. V

processing of personal data[53]. For the same reason, the Directive requires the involvement of work councils/representatives: they are to be informed in advance and express their opinion before the introduction of workers' control and monitoring methods. In order to enable or facilitate access to data, the Greek Authority considers as necessary the possibility of the employees to be assisted in the exercise of their rights by a specialist or a worker representative.

4. Sanctions, Compensations and Legal Consequences

[60]. Greek Data Protection law provides for judicial remedies and the civil liability of the data controller in case where a person has suffered damage as a result of unlawful processing. The starting point of the legislator's approach was that the existence of effective and dissuasive sanctions is important in ensuring respect for the adopted rules. Therefore the law includes an impressive array of detailed provisions on sanctions, which may be administrative or criminal, in case of non-compliance with the provisions of the law.

[61]. As far as administrative sanctions are concerned, the Authority may impose on the Data Controllers sanctions for breach of their duties arising from this law as well as from any other regulation on the protection of individuals from the processing of personal data. The provided sanctions are a) a warning with an order for the violation to cease within a specified time limit, b) administrative fines ranging from 880 Euros to 146.735 Euros, c) temporary or definitive revocation of the permit and/or the destruction of the file or a ban of the processing and the destruction, return or locking of the relevant data. These sanctions can be imposed also cumulatively. The administrative sanctions provided in Art. 21 of the Law 2472/97 may be also imposed in cases of breach of the provisions concerning the personal data and privacy protection in the electronic communications sector[54].

[62]. Such sanctions are commensurated to the gravity of the violation impeached. The law provides that the revocation of a permit or the destruction of the file/database should be imposed in case of a particularly serious or repeated violation. The Authority has until now

[53] An approach adopted also by the European Commission in the Report: Possible content of a European framework on protection of workers' personal data, Brussels 2002.

[54] As explicitly stated in Art. 13 § 4 of the Law 3471/06.

refrained from imposing the highest fines allowed by the law. Only in few cases the DPA has imposed high fines on media enterprises, banks and insurance companies.

[63]. 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[55]. The Authority places emphasis on the symbolic value of such a sanction[56] imposing relatively low fines.

[64]. The law provides for penal sanctions in case of non-compliance with a) the substantial and procedural provisions of the law and b) the binding decisions of the Data Protection Authority. In the first case, penal sanctions can be imposed to anyone[57] who a) keeps a file without notifying the DPA, b) keeps a file without permit[58] of the DPA, c) proceeds to interconnection of files without notifying the DPA, d) transfers personal data in breach of the legal provisions[59]. Penal sanctions may also be imposed in case of breach of rules of lawful processing as well as security and secrecy legal requirements[60].

---

55 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.

56 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.

57 In this case it is "anyone" who is punishable and not only the Data Controller or the Data Processor.

58 This is the case of processing of the so-called "sensitive data", the processing of which is lawful upon the conditions of Art. 7 and it is subject to prior control and permit granted by the Data Protection Authority.

59 Penal sanctions are provided also for the case that data is processed in breach of the terms and conditions, which the DPA has set by granting a permit.

60 According to Art. 22 § 4, anyone who unlawfully interferes in any way whatsoever with a personal data file or takes notice of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorised persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment and a fine and, regarding sensitive data, by imprisonment for a period of at least one (1) year and a fine amounting between 3.000 and 30,000 Euros unless otherwise subject to more serious sanctions. This provision has been strongly criticised as it introduces an extensive penalisation of the informational behaviour and violates the foreseeability criterion (lex certa criterion). On the other side, it has been

[65]. Criminal sanctions range from imprisonment of up to one year for keeping a file without permit or for breach of a permit's conditions to incarceration of ten years for anyone who by breaching the provisions of the law purported to gain unlawful benefit on his/her behalf or on behalf of another person or to cause harm to a third party. These sanctions may be coupled with (penal) fines amounting between 2.934 Euros and 29.347 Euros.

[66]. Law 3471/06 lays down more severe pecuniary sanctions (fines) for anyone who unlawfully interferes, in any way whatsoever, with personal data of a subscriber or user, or takes notice of such data or extracts, alters, affects, destroys, processes, transfers, discloses, makes accessible to unauthorised persons or exploits such data: in this case the fine may reach the amount of 100.000 Euros and if the unlawful processing or the confidentiality breach endangers the free operation of democratic constitution or national security the judge/court may impose a fine up to 350.000 Euros.

[67]. As far as it concerns penal liability the law provides that if the acts of a) keeping a file without notifying the DPA or without its permit of the DPA, b) proceeding to interconnection of files without notifying the DPA, c) transferring personal data in breach of the legal provisions and d) breaching the rules of lawful processing as well as security and secrecy legal requirements, were committed as a result of negligence, then the sanctions to be imposed are milder (imprisonment for a period of at least three (3) months and a fine) The accused person has to prove that the breach of the law was committed by negligence.

[68]. The law provides for the civil liability for pecuniary or non-pecuniary (moral) damage. Any natural person or legal entity of private law, which in breach of the provisions of the law causes pecuniary damage, should restitute the damage in full. According to Art. 23 of the Law 2472/97 "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.[61] 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).

---

argued that such actions could have a dissuasive effect on the unlawful and unfair processing of data.

61 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.

[69]. The moral damage, i.e. the grief caused to a person, which cannot be assessed in money, is satisfied with an allotment of money[62]. Moral damages are restituted only when the law so stipulates. Such is the case of an unlawful act (art. 932 Civil Law). The compensation payable according to article 932 of the Civil Code for non pecuniary damage caused in breach of the Law 2472/97 is set at the amount of at least 5.869 Euros, unless the plaintiff claims a lesser amount or the said breach was due to negligence. In the latter case, the person who caused the damage has the burden to prove that he didn't want or accept the result, i.e. the breach of the law concerning data protection. Such restitution shall be awarded irrespective of the claim for pecuniary damages.

[70]. As far as it concerns civil liability in general: with delictual liability the burden of proof of all actual facts which make up the conditions for the claim (i.e. also the fault) is borne by the injured party, in accordance with the general procedural rule that the burden of proof lies on the plaintiff. In relation to the civil liability provided in Greek Data Protection Law it is 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.

[71]. The claims are litigated, notwithstanding whether the Authority has issued a relevant decision or whether criminal charges have been brought or suspended or postponed on any grounds whatsoever. Due to the separation of powers principle, the Authority is not involved in the civil or penal procedure. The DPA has the competence to bring violations of the law to the attention of judicial authorities for further investigation. The Authority makes use of this possibility but it does not necessarily pursue the case.

[72]. However, enforcement of data protection legislation through penal sanctions and/or civil liability depends mainly on personal initiative of the affected data subjects. The DPA informs data subjects about their rights embedded in law either through informational material or through responses to petitions and questions and occasionally through personal consultation but it does not assist data subjects in a formal and official manner, i.e. through legal representation or assistance in court proceedings. The procedural costs and court/attorney fees are carried accordingly to the general procedural rules and they are defined by the competent Court, which tries the civil/penal case. Legal assistance is provided according to general provisions of the law in very exceptional cases.

[62] The reason for restituting moral damage is to alleviate the emotional pain of the person that was harmed and to comfort him psychologically. More about in P. Agallopoulou, Basic concepts of Greek Civil Law, Athens-Bruxelles-Berne 2005, p. 206 ff.

[73]. The protection of personal data in the employment sector is ensured through the application of data protection rules as interpreted by the Directive 115/2001 of the DPA. The latter provides the involvement of work councils/representatives before the introduction of workers' control and monitoring methods. According to the same Directive employees may be assisted in the exercise of their rights by a specialist or a worker representative. With the exception of abovementioned possibilities no provision is made for an institutional role for the collective bodies representing the workers or for their ability to intervene effectively. The only regulation and initiative concerning collective bargaining refer to the national level. Specifically Article 17 of the 2001-2002 EGSSE (the National Work Collective Agreement) regarding protection of personal integrity states that the contracting employer organisations underscore to their members the obligations for enterprises arising from the legislative framework as regards the protection of the individual relative to matters of a personal nature, aimed at protecting workers' personal integrity. The social partners have not yet devoted attention to the question of protection of and respect for privacy/private life in the workplace on any level. This question is completely absent from the agenda of dialogue between the two sides and from the unions' framework of demands; neither the employer organisations nor the trade unions have developed a framework of positions/proposals.

5. Rights awareness

[74]. With the exemption of the first phase[63] the Greek Data Protection Authority has not initiated powerful and long-term awareness raising campaigns. Given the Authority's mission to encourage privacy culture among data controllers and to educate them the DPA has mainly tried and is still trying to raise awareness among the data controllers - with an emphasis on the public sector - by organising seminars or participating in educational activities organised by the public and private sector.

[75]. Since 2002, the DPA has focused its efforts for informing the public through its presence on the web[64]. On its renewed website (www.dpa.gr) the Authority has published a lot of information material, including brief analysis of the legal instruments, the rules governing specific files and sectors, FAQs and the potential source of problems for data subjects. Data subjects thus have a better picture of

[63] The DPA has produced a video and leaflets, which have been broadly distributed. See Annual Report 1999, p. 17 ff.

[64] See Annual Report 2002, p. 57 ff., Annual Report 2007, p. 39 ff.

their situation and are better able to take action vis-à-vis either the controller or the DPA.

[76]. The DPA considers that the growing number of data subjects' complaints and petitions is not –necessarily - evidence of non-compliance and/or increased number of violations of the law. It is merely considered as the result of subject's self-consciousness and the growing awareness among the public and the data protection specialised lawyers. The complaints investigated concerned mainly the bank sector and the public sector[65]. A great number of complaints relate also to direct marketing through unsolicited calls and spam cases.

[77]. An overview of the requests and complaints shows that data subjects increasingly refer their cases to the DPA following either an unfavourable administrative decision or a decision and/or a measure taken by a private person which affects specific rights and interests of the data subject in a given –mostly contractual- relationship (employee-employer relationships, bank and bank customers, assurance companies)

[78]. Data subjects do not lack alternatives for enforcement of their rights, as they have the possibility to seek judicial protection. However, even if seeking help from the DPA is neither the only one nor a compulsory step before taking further legal action, the vast majority of lawyers specialised in data protection issues choose either to appeal the case before the DPA or to follow both procedures (DPA and civil/penal Court). Especially during the first years of the data protection law enforcement, the civil courts have in several cases suspended the court proceedings/judgement waiting for the opinion and/or the decision of the Authority.

[79]. At the beginning most people were confused both about the application of the law and about the powers granted to the Authority. The initial approach/attitude to the new regulation was a mixed one: it ranged from indifference to great expectations that the DPA would prohibit the collection and processing of data in general. There are 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. According to a recent survey[66] 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

[65] See Annual Report 1999 p. 16, Annual Report 2001 p. 22 ff.,

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

independent authorities[67] as far as it concerns the trust that the citizens have in the Authority.[68] 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%).

[80]. 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[69] 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)[70] 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[71].

[81]. The media have covered the activities of the Authority in a satisfactory manner[72]. Media have improved rights awareness by reporting breaches of the law and the measures taken by the DPA especially in cases which affect potentially a lot of people, like non-compliance in the employment sector or use of CCTV systems in private places. In relation to some famous cases, the Authority has been criticised from a part of media and public opinion that "it has resisted against the revelation of a paedophile singer"[73] or that "it has offered protection to people who breach the law"[74].

---

67 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).

68 For more information see www.publicissue.gr

69 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.

70 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.

71 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).

72 See for example Annual Report 2005, p. 111ff. However, with the exemption of the first phase, the DPA's Presidents and Members avoid to have a direct relationship with the media, using press releases as the sole means to communicate their decisions and opinions.

73 By imposing fines on a journalist and a TV-channel, which projected a video containing strictly private erotic scenes of a famous Greek singer.

74 By regarding that the revelation of the names of persons who are suspect or accused for a crime, without being yet convicted, is an interference with the right to privacy and data protection and should be allowed only in exceptional cases and for the purpose of facilitating law enforcement.

[82]. Actually there are very few intermediary organisations, like NGOs or trade unions active with data protection, which could serve as partners or allies in the execution of the DPA's tasks and duties. A consumer's union (ΕΚΡΟΙΖΟ) has initiated legal actions in the interest of its members focusing on contract terms (in bank sector) that relate to the collection and secondary use of customers' personal data. Another active NGO is one consisting mainly of attorneys and lawyers[75], which focuses on issues pertaining to video surveillance in public places[76]. On the other side, the Authority seems to be not so extrovert. The DPA has refrained from systematically encouraging alliances with NGOs.

6. Analysis of deficiencies

[83]. From a fundamental rights perspective a main deficiency of the regulatory framework consists exactly in 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[77]. This last amendment of the law ignores the "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 constitutional framework[78].

[84]. Moreover, specific international legal instruments stress the need for an effective supervision and inspection by an independent authority of the processing of personal data especially in the police sector.[79] Informational exchanges and cooperation among the national security

[75] It concerns the NGO "Democratic Coiling for Freedoms and Solidarity" (Δημοκρατική Συσπείρωση για τις Λαϊκές Ελευθερίες και την Αλληλεγγύη).

[76] This NGO has applied for the annulment of the DPA's decision on video surveillance in public places for security purposes. They argue that the DPA has been too permissive concerning the use of CCTV system even for traffic control.

[77] This exclusion has been introduced through Art. 8 of the Law 3625/07.

[78] 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.

[79] See for example the Europol Convention (Art. 11, 14) or the Additional protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS No. 181, in combination with Recommendation No R (87) 15 regulating the use of personal data in the police sector.

and police authorities[80] presuppose the oversight of their activities by independent authorities. In addition, Art 16 of the Treaty on the Functioning of the EU includes a subjective right to data protection and clearly affirms that compliance with data protection rules shall be subject to the control of independent authorities. The supervision by an independent Authority is a guarantee that art. 8 of the Charter of Fundamental Rights spells out as an essential element of the right to data protection. In this perspective, this last modification of the law constitutes a breach of legal provisions, which are binding for the national legislator and public authorities.

[85]. A second major problem concerns the transparency and consistency of the legal framework concerning data protection in the electronic communications sector. The existence of at least four laws that are simultaneously applicable[81] and of two Authorities, which have in some areas overlapping competencies, raises a lot of problems concerning the effective and consistent application of the respective rules. This confusing situation has also a wide-ranging impact on the addressees of the legal requirements, i.e. the service and network providers who pretend that this lack of clarity impedes them from evolving a practice and a culture of compliance.

[86]. A revision of the legal framework in order to improve its consistency and ensure its applicability of the legal framework pertaining to privacy, secrecy/confidentiality and security in the electronic communications sector is apparently and urgently needed. Such a review (or codification) of the entire legal framework should also comprise a re-allocation, a re-set of (the boundaries between) the

[80] See for example the Council Decision 2007/533/JHA for the establishment, operation and use of the second generation Schengen Information System II or the Proposal for a Council Framework Decision on the organisation and content of the exchange of information extracted from criminal records between MS [COM 2005 (690)].

[81] Concretely: Law 3471/06 on the protection of privacy and personal data in the electronic communications sector contains –among others - provisions pertaining to the processing of personal data (including traffic data), the secrecy/confidentiality of communications data (content/traffic data) and the security of data, systems and networks. According to Art 3 § 2 Law 2472/97 shall apply – as "general law" to all matters that are not regulated explicitly by Law 3471/06. The monitoring of compliance with these laws falls under the competence of the Data Protection Authority. However applicable is also Law 3115/03 on Hellenic Authority for the Information and Communication Security and Privacy, which is responsible for the assurance of secrecy in the electronic communications sector and understands its competence as encompassing also the whole range of networks security and every art and phase of data processing, which is related to communication. The confusion has been deepened with the recent adoption of the Law 3674/08 on the assurance of telecommunications secrecy that allocates further competences to the Hellenic Authority for the Information and Communication Security and Privacy while referring also some competences of the DPA and it will grow worse with the transposition of the Data Protection Directive, as both authorities will probably have overlapping competences concerning the security of the retained traffic data and the monitoring of the use of these data during the retention period.

competences of the Data Protection Authority and the Hellenic Authority for the Information and Communication Security and Privacy.

[87]. All supervisory authorities act, variously, as ombudsmen, auditors, consultants, educators, negotiators, policy advisers, enforcers and international ambassadors. Not every role is played with equal weight by every commissioner. Every data protection authority needs to consider how these various tasks and roles are to be performed. As a public authority and under the general constitutional and administrative law, the DPA is obliged to respond to petitions, requests and complaints[82].

[88]. As many other supervisory authorities, the Greek DPA presently suffers because its activity is dominated by individual complaints. With one of the last amendments of the law (2006) there was an attempt to face this problem by enabling the Authority to file applications or complaints, which are deemed broadly vague, unfounded or are submitted inappropriately or anonymously[83].

[89]. However, the Authority is obliged to deal with all complaints and requests for assistance, without the possibility to exercise a reasonable discretion as to whether and how to deal with the issues. The increase in the number of claims has caused backlogs and other problems. It leads sometimes the Authority to concentrate its efforts on those issues it receives most complaints and questions about which may not necessarily be the most significant issues affecting data subjects and the democratic society as a whole. In the interior of the Authority there is a strong feeling of being overwhelmed by complaints, of being unable to manage them in a reasonable time span, of being regarded by the citizens as the last resort or as a sort of single court.

[90]. The Authority perceives the increased workload as disproportionate to the limited human resources. The DPA seems that it has neither the institutional nor the organisational ability to choose whether to emphasize individual or structural aspects in complaints. In some cases there is a recognisable effort to formulate the decisions in such a way as to create a precedent but such an approach is not easy, as the Authority is focused on the legal remedy to be provided to an

[82] According to Art. 10 of the Greek Constitution, each person shall have the right to petition in writing public authorities, which shall be obliged to take prompt action in accordance with provisions in force, and to give a written and reasoned reply to the petitioner as provided by law.

[83] See Art. 19 §1 m of the Law 2472/97

individual[84].The number of complaints limits inevitably the capacity of the Authority to invest sufficient resources in important issues and activities[85]. Individual cases dominate the agenda at the expense of other matters and mainly the pro-active audit and the regulatory activities of the DPA.

[91]. The powerful statutory panoply possessed by the independent authority does not in itself guarantee the effectiveness of compliance control and, in a final analysis, of protection. It may, instead, prove to be its "Achilles' heel". The effectiveness of control is cancelled if the Authority arrives at a rationale of standard procedures and its control operation becomes entrapped in a function of providing permits, as if it were a kind of motor vehicle inspection issuing "certificates of protection of personal data".

[92]. The effectiveness of the Authority seems to be considerably affected also by the situation of the staff. The personnel of the Authority (including Auditors) are public officials. The fact that the officials of the DPA are paid less than their colleagues in other independent authorities results in major difficulties relating to the -in any case restricted - possibility of the Authority to attract in the long term specialized and committed staff. A further consequence of their organisational and financial status in combination with the increased tasks is a lack of motivation among the staff[86].

[93]. The Authority intends to face these problems by proposing the adoption of legislative measures pertaining to a) the status of the Members of the Authority[87], b) the improvement of the status of the staff, c) the increase of the number of officials, d) the re-organisation of the Authority and especially with regard to the possibility to convene and decide not only in plenum but also in Chambers/Divisions. These measures, if adopted by the legislator, could contribute to a better functioning of the DPA and consequently to a more effective implementation of the law.

---

84 This approach is explained by the obligation to reply to requests but it approach seems to be in addition influenced by the fact that all the Chairmen (former and present) of the Data Protection Authority were Judges of highest rank as Art. 16 of the Law 2472/97 requires that a judge if a rank corresponding to that of a Counsellor of State (Conseiller d' Etat) is to be appointed as President of the Authority.

85 The difficulties caused by the increasing number of complaints was a common finding of both the former President D. Gourgourakis and the present President of the DPA Christos Geraris. The problem of the accumulation of complaints and petitions/questions has been also publicly raised during the presentation of the last Annual Report of the Authority. See Press Release at www.dpa.gr

86 See Annual Report 2005, p. 19 ff., Annual Report 2006, p.20 f.

87 Only the President of the Authority is engaged on a full-time basis. The proposal of the Authority will be to amend the Law in order to engage all (7) or the majority of the Members (4/7) on a full-time basis.

[94]. Apart from the exemption of the police sector from the scope of application the Greek legal framework could be regarded as adequate enabling an effective implementation. The setting-up of the Data Protection Authority and the organisation of the law monitoring is probably the most important pillar of the Greek law. In the final analysis the effectiveness of the substantive regulations depends upon the quality and mode of operation of the Authority.

[95]. It is difficult per se to commit effective tasks to a data protection authority by identifying areas of competence and sectors of activity that would otherwise be reserved for judicial authorities, other public bodies and/or an Ombudsman. The Data Protection Authority should be independent, authorative, professional, effective and be able to interact with the other institutions and capable, at the same time, of coping with possible conflicts arising in respect of public and private entities. A basic inherent problem, which the Authority must deal on a daily and at the same time on a long-term basis, is how to fulfil its constitutional/institutional duties while avoiding its decline into bureaucracy[88]. Another major challenge is how to combine in a balanced and effective way the role of an informational Ombudsman with that of a political institution for control and dialogue with the state and the citizens on the developments in technology and its applications, and their effects on freedoms and on the organisation of state, society and economy. Dealing with every-day burdensome activities, the Greek Authority did not have the opportunity to develop a general and long-term plan on how it could encourage a culture of compliance and more generally of privacy protection throughout the society, the economy, and government in an era of widespread adoption of privacy-invasive information technologies.

[96]. The Greek DPA has adequate powers of investigation and effective powers of intervention. The Authority is granted with sufficient powers and not negligible resources. It should use them in a selective and pragmatic manner, while concentrating at serious and likely harms or main risks. Its future as an independent agency will depend more on a clear understanding of its role and its own capacity to fulfil a number of conditions that are crucial for its effectiveness.

[97]. However, the socio-political context could not be considered as favourable. The data protection requirements as well as the data protection authority were and still remain actually a "novelty" in the Greek institutional system. The right to data protection is often evoked

[88] The Authority has already in the Annual Report 2000 stressed the risk to decline into a bureaucratic organisation, as the burdensome routine work would prevent it from intervening in major data protection issues and debates. See Annual Report 2000 p. 11 ff.

either as pretext for hindering access to information[89] or as "scape-goat" for shortcomings and inefficiency of public authorities.

[98]. In addition, lawyers[90] and politicians[91] often question the role and importance of the DPA. There is a debate in progress concerning the existence of "too many independent authorities" as well as their independence and accountability. Criticisms of the delegation of substantial power to DPA rely on the lack of democratic legitimacy and parliamentary scrutiny. This argumentation, which flows from traditional legal doctrines of modern representative democracy regarding the rule of law and the separation of powers, ignores or underestimates a) the fact that the acts of the Authority are to be scrutinised by the Council of State and b) their obligation to report to the Parliament. However it may undermine the effectiveness and the integration of the DPA into the institutional-political system as a guarantor of the democratic rule of law.

7. Good Practice

[99]. Actually it has not been possible to identify practices, which have been recognised as and/or could be considered as "good practice" regarding effective data protection measures. Data protection is a relatively new legislative material, which has not yet been integrated in the practice of public and private organisations. In addition, the data protection system has been structured in such a way that the Authority is pivotal for the enforcement of the relevant provisions, which may "serve" as an excuse for not taking initiatives to evolve good practices.

[100]. The Greek legislation provides for the possibility of adoption of codes of conduct, although there is no specific article included in the data protection act. 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

[89] Often, many public authorities do not comply with their information duties pretending that they are not allowed by the data protection legislation to give access to information. This position has also far reaching consequences in relation to the transparency of the administrative action.

[90] See S. Meglidou/F. Kozyris (Eds), The independence of the Independent Authorities, Athens-Komotini 2003. Also Kosmides, Zehn Jahre griechisches Datenschutz: eine kritische Bilanz, Datenschutz und Datensicherheit DuD 1/2008, p. 19 ff.

[91] See A. Psarouda-Mpenaki (former President of Parliament), The independent Authorities in the state system, in N. Frangakis (Ed.), The Independent Authorities in Modern Democracy, Athens-Komotini 2008, p. 14 ff.

freedoms of persons in their field of activity. It is not clear if these codes of conduct should be submitted to the Data Protection Authority or approved and registered by it.

[101]. In any case, self-regulation is regarded in Greece 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)[92].

[102]. Finally, as "good practice" could be considered the sporadic efforts to introduce a kind of "privacy by design approach " or – more correctly – to "reward" private companies for proposing privacy-friendly IT-systems when participating to public procurement procedures in the Framework of the Operational Programme "Information Society". However, this attempt has not been continued.

8. Miscellaneous

[103]. Nothing to report.

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

Annexes

Annex 1 - Tables and Statistics

Please complete the table below

	2000	2001	2002	2003	2004	2005	2006	2007
Budget of data protection authority	481.000.000,00 GRD	502.500.000,00 GRD	950.154,38 EUR	1.699.575,00 EUR	1.675.000,00 EUR	1.900.000,00 EUR	2.266.348,00 EUR	2.708.920,00 EUR
Staff of data protection authority	The President, the Deputy President, 6 Members and 6 Alternate Members of the	The President, the Deputy President, 6 Members and 6 Alternate Members of the	The President, the Deputy President, 6 Members and 6	The President, the Deputy President, 6 Members and 6 Alternate	The President, the Deputy President, 6 Members and 6 Alternate	The President, the Deputy President, 6 Members and 6 Alternate	The President, the Deputy President, 6 Members and 6 Alternate	The President, the Deputy President, 6 Members and 6 Alternate

	Authority, 25 employees	Authority, 23 employees	Alternate Members of the Authority, 23 employees	Members of the Authority, 23 employees	Members of the Authority, 25 employees	Members of the Authority, 29 employees	Members of the Authority, 44 employees	Members of the Authority, 40 employees
Number of procedures (investigations, audits etc.) initiated by data protection authority at own initiative	14	15	9	5	36	22	17	19
Number of data protection registrations	65000	990	238	283	415	202	251	560

Number of data protection approval procedures	165	195	74	279	323	174	102	110
Number of complaints received by data protection authority	729	663	1023	236	626	816	1095	1054
Number of complaints upheld by data protection authority	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Follow up activities of data protection authority, once	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

problems were established (please disaggregate according to type of follow up activity: settlement, warning issued, opinion issued, sanction issued etc.)								
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	N/A	Sanctions 13 fines, 10 warnings, 04 deletion of data, 02 destruction of file/ban of processing Recommendations: 15	Opinions: 07 Sanctions 05 fines, 18 deletion of data, 03 destruction of file/ban of processing	Sanctions 11 fines, 07 deletion of data Recommendations: 07	Opinions: 03 Sanctions 12 fines, 21 deletion of data, 02 destruction of file/ban of processing Recommenda	Sanctions 15 fines, 17 deletion of data, 04 destruction of file/ban of processing Recommendations: 15	Opinions: 02 Sanctions 22 fines, 42 deletion of data, 14 destruction of file/ban of processing Recommenda	Opinions: 01 Sanctions 18 fines, 41 deletion of data, 08 destruction of file/ban of processing Recommendations: 19

between sectors of society and economy)			Recommendations: 14		tions: 18		tions: 29	
Range of sanctions and/or compensation in your country (Please disaggregate according to type of sanction/ compensation)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

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

Annex 2 – Case Law

Case title	Case Triantafyllopoulos
Decision date	31.01.2000
Reference details	Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)
Key facts of the case (max. 500 chars)	Broadcasting of erotic scenes in which a famous singer was involved in sexual intercourse with a juvenile person, whose image was not identified, and reading of extracts from a personal diary with parallel of the relevant pages, with text and photographs of half-naked men in which reference was made to actions of sexual nature with persons of the same sex whose names were explicitly mentioned.
Main reasoning/ argumentation (max. 500 chars)	The possession, recording in a file and use on TV of pictures of sexual life are subject to the meaning of processing of Law 2472/97, given that they constitute in any case use or dissemination of personal data. From the Constitution the predominance of freedom of information over the right to informational self-determination and the dignity of person does not arise in abstracto. The use of sensitive data of such character during broadcasting programmes constitutes processing that exceeds the limits imposed from the constitutionally consolidated principle of proportionality, also directly consolidated in the framework of article 4 par.1b, Law 2472/1997.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	By this case the DPA clarified that the use of pictures is a form of processing of personal data, falling under the scope of the law. The competence of the DPA and this of the National Council for Radio and Television coincide in this case.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Ban of processing and destruction of files: Sanction imposed on to 'SATELLITE TV ALPHA SA' and the "E. TRIANTAFYLLOPOULOS and CO SA" TRIANTAFYLLOPOULOS takes possession of it. Fine of 58.694 € to the journalist E. Triantafyllopoulos, Fine of 29.347 €) to "SATELLITE TELEVISION ALPHA SA"
Proposal of key words for data base	Privacy, Dignity, Freedom of Information, Sensitive Data, Competence of DPA

Case title	Case Identity Cards
Decision date	15.05.2000
Reference details	Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)
Key facts of the case (max. 500 chars)	Following a petition of Mr. S. Manos, Independent MP, the Minister of Justice M. Stathopoulos asked for the opinion of the DPA in relation to the compliance of the content of IDs with the provisions of the Data Protection Law.

Main reasoning/ argumentation (max. 500 chars)	Identity cards constitute public documents containing personal data. In view of the purpose of processing being the verification of the identity of the data subject the following data, i.e. a) fingerprint, b) spouse's name c) profession, d) residence and e) religion are deemed not to be necessary and proportionate. As far as it concerns religious beliefs, this data refers to the inner world of the individual and it is therefore neither appropriate nor necessary in order to prove one's identity.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Act 2472/1997, being new and containing provisions that introduce in the Greek law and order regulations of supra-legislative validity pertaining to the international and community law, imposes the interpretation and implementation of previous regulations concerning identity cards according to the stipulations and the principles therein. The processing of the data is unlawful even if the data subject has given his/her explicit consent according to Act 2472/1997, articles 5 §1 and 7 §2 section a of, since the data subject's consent does not allow for any form of processing when unlawful or contrary to the principles of purpose, necessity and proportionality in stricto sensu.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The DPA warned and invited the Ministry of Public Order (controller) and any other relevant body to comply with the content of this decision in due time and in any case not later than necessary in order that the pertinent procedures be adapted by issuing all necessary directives and forwarding them to the competent authorities and bodies
Proposal of key words for data base	Identity cards, fingerprints, religious beliefs,

Case title	61/2004 (employees' monitoring)
Decision date	17.11.2004
Reference details	Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)
Key facts of the case (max. 500 chars)	The case involved the operation of a Virtual Network Computing (VNC) system, which allowed access to the employees' personal computers and monitoring of their communications. The system provided the IT department with access to view the employees' PC screens and storage spaces and operate their computers by remote control. The company's IT department retained copies of all e-mails for an indefinite period of time and monitored website visits "for statistical purposes".
Main reasoning/ argumentation (max. 500 chars)	Both the real time monitoring of employee activity and access to data stored in his/her computer falls under the definition of personal data processing. As regards the record of web pages visited by employees kept for statistical purposes, such record amounts to violation of the principle of proportionality. From the same principle emanates the prohibition of the general, systematic and pre-emptive collection and recording of data on Internet use.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The remote access to computer data and processing constitutes processing of personal data. The generalized and systematic monitoring of Internet use infringes the rights to communicational privacy and data protection and violates the principle of proportionality.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Authority addressed a warning to the employer to proceed to the following actions: information of employees, use controllable by employees, storage space not accessible by third persons (including the employer), refraining from systematic monitoring and recording of electronic communications and Internet use
Proposal of key words for data base	Employees' privacy, e-mail monitoring, Internet use monitoring, remote access to employee's equipment, information duties

Case title	150/2001 (Unlawful disclosure and secondary use for advertising purposes)
Decision date	11.12.2001
Reference details	Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)
Key facts of the case (max. 500 chars)	By a complaint the complainant stated that upon his wife's delivery in a Maternity Clinic, he began to receive repeated unsolicited calls from insurance agents of the an Insurance Company in order to be informed on insurance policies for the newborn. They lodged complaints against the Maternity Clinic and the Insurance Company for an illegal use of their personal data, stating that their personal data were never given for advertising or other similar purposes.
Main reasoning/ argumentation (max. 500 chars)	The maternity clinic did not abide by the necessary organizational and technical security measures with the consequence that, its employees, acting obviously for their own personal benefit, access illegally the file, acquire personal data recorded in it and forward them illegally to third parties. The insurance company is responsible for the intentional unlawful processing of personal data of its agent.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Controllers are responsible also for the unlawful collection of personal data. Controllers (in this case the insurance) are held responsible about the way its agents (processors) work, even they claimed that they are not aware of the source of data which the persons carrying out this processing had at their disposal.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	A fine of five million drachmas 14.673,51 Euro to the insurance company for the illegal processing of personal data A fine of one million drachmas 2.934,7 Euro to the maternity clinic for omitting to take technical and organizational measures, resulting in the leak of the complainants' personal data.
Proposal of key words for data base	Unlawful disclosure, Secondary use, advertising, security, controller, processor

Case title	62 / 2003
Decision date	12.12.2003
Reference details	Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)
Key facts of the case (max. 500 chars)	"TEIRESIAS Ltd" (a company controlled by the Hellenic Banks Association, acting as credit reporting agency), had asked for the amendment of previous decisions of the DPA, so that credit insurance and security guarantee companies can also be recipients of the information it keeps.

Main reasoning/ argumentation (max. 500 chars)	The purpose of processing the file kept by "TEIRESIAS Ltd" rests in minimizing the risks from concluding credit contracts with un-creditworthy clients and in general from creating insecure demands and finally in protecting the commercial value and improving economic transactions. Insurance of credits and guarantees from insurance companies implies the risk of un-creditworthiness of the debtor.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The Decision refers to the strict purpose limitation of processing. Financial services activities/ companies do not constitute an entity, where personal information can be circulated and disclosed freely.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Extending the recipients of the file of "TEIRESIAS Ltd" to Credit and Guarantee Insurance Companies has not be considered as justified by the purpose of process of the specific file and is therefore not legal.
Proposal of key words for data base	Creditworthiness, financial services, insurance companies, purpose limitation

Case title	52 / 2003
Decision date	05.11.2003
Reference details	Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)

Key facts of the case (max. 500 chars)	The notification concerns a European-level project in which participate IAA, the International Air Transport Association (IATA), the International Airport at Milan, ALITALIA Airlines and International Airport of Athens. The basic aim of the project is the establishment of a biometric model for identity verification of registered passengers during departure from airports. The pilot implementation of the biometric system in Milan and Athens airports for a period of about 6 months is set up on a voluntary basis for the evaluation of various aspects of the chosen technical solution. In particular, the implementation of the biometric system in check-in and boarding points aims at guaranteeing that the passenger who has checked in is the same with the person, who actually boards the airplane.
Main reasoning/ argumentation (max. 500 chars)	Biometric data processing for the identification of persons for the pilot implementation of the project notified by IAA, examined under the principles of purpose and necessity, is not lawful. The purpose sought with the biometric method can be achieved in a milder way with the passenger showing the identity card along with the ticket and the boarding card. the method provided for by the pilot project does not mainly serve flight security requirements but organisational issues of airline companies instead.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The processing of biometric data falls under the scope of the Law. Such data must be processed for specific purposes. Biometric data processing for security purposes has to be assessed under the criterion of proportionality principle. The fact that participation is voluntary does is not of importance, if the mentioned processing is deemed to be non compliant with proportionality principle.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	Biometric data processing for the pilot implementation of the project notified has been considered as unlawful and, therefore, the collection and processing of iris and fingerprint data in IAA for the verification of identity of future passengers has not been permitted by the DPA.
Proposal of key words for data base	Biometric methods, identity, security, proportionality

Case title	58 / 2005 (CCTV in public places)
Decision date	12.08.2005
Reference details	Hellenic Data Protection Authority (Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα)
Key facts of the case (max. 500 chars)	The Ministry of Public Order requested from the Authority to extend a) the time period of the operation of the CCTV used for the monitoring traffic and b) purposes of collection/processing through CCTV equipment, including safety and security purposes (prevention-investigation of crimes, crisis management, protection of vulnerable targets).
Main reasoning/ argumentation (max. 500 chars)	Recording and processing of personal data through a CCTV system operating on a permanent, continuous or regular basis, is prohibited, because it infringes on the individual's personality and privacy. Video monitoring restricts freedom, and hinders the free development of social and political activity. The lawfulness of processing is examined on the basis of the principle of proportionality. The efficiency of CCTV in public places in connection with the prevention or the repression of acts that are detrimental to public safety could not be concluded from the request. Upon specific and in case of an exceptional and special need the DPA could grant a permit.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Video-monitoring is a form of processing, irrespective of the storage of the data in a file.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The DPA accepted, under terms and conditions, the use of CCTV systems only for traffic monitoring.
Proposal of key words for data base	CCTV, public places, traffic monitoring, security, safety, proportionality

Case title	2629/2006
Decision date	26.11.2006
Reference details	Council of State (Συμβούλιο της Επικρατείας)
Key facts of the case (max. 500 chars)	The Ministry For National Defence has notified the DPA its intention to publish the names of persons who, due to the condition of their health, were deemed to be not liable for military service. The DPA has not opposed to the investigation of cases of deception and/or corruption but it did not allow the publication of the names, as it would infringe the proportionality principle. As legal ground/purpose the Ministry has invoked the need to fulfil public interest and demonstrate that such practices are contrary to the said interest. The Ministry filled an application for annulment of the Decision of the DPA.
Main reasoning/ argumentation (max. 500 chars)	The administrative acts, by which the persons were found non liable for military service, are deemed lawful, as long as they are not annulated. Therefore, the publication of sensitive personal data (even of is not founded on the provisions of the Law, which allows the processing of such either for the purposes of national security and/or detection of crimes/offences, which is not the case.

Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Publication of data is a form of data processing. Processing of sensitive data is lawful if founded on specific legal grounds provided.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Council of State upheld the Decision of the DPA
Proposal of key words for data base	Processing, sensitive data, public interest

Case title	1367/2008
Decision date	06.05.2008
Reference details	Council of State (Συμβούλιο της Επικρατείας)
Key facts of the case (max. 500 chars)	The DPA has imposed a fine on a private commercial company for unlawful processing, which consisted in collecting/processing data of a person and sending a letter to it concerning the organization of a conference, taking place during a cruise. The recipient was inserted to the register with identification data of people, who do not wish their data to be processed for direct marketing purposes ("Register of Art. 13"). Advertisers should consult this register and refrain from data processing. The company has filled an appeal for annulment of the Decision of the DPA.

Main reasoning/ argumentation (max. 500 chars)	The Company has sent the advertising letter, after having collected, processed and assessed personal data of the recipient and keeping a respective file in the meaning of the law. The DPA imposes fines for breach of the duties laid down in law. By deciding the sum of a fine the DPA has not to take into account the damage/potential damage caused to data subject.
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	Advertising mailing cannot be disconnected from processing of personal data, which serves as basis for the direct marketing/advertising activity
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Council of State upheld the Decision of the DPA
Proposal of key words for data base	Direct marketing, Processing of personal data, moral damage

Case title	1770/2005
Decision date	24.11.2005
Reference details	Court of Cassation [Civil/Penal Supreme Court (Άρειος Πάγος)]
Key facts of the case (max. 500 chars)	The DPA maintains a register with identification data of people, who do not wish their data to be processed for direct marketing purposes ("Register of Art. 13"). Advertisers should consult this register. A person who was inserted (since 1999) in the Register of Persons has received advertising mailings from a private

	company. He took legal action and asked for restitution of the moral damage caused to him through repeated advertising mailings. His sue for restitution of moral damage was rejected both of the Courts of 1st Instance and the Court of Appeal. He took the case to the Civil/Penal Law Supreme Court (Court of Cassation)
Main reasoning/ argumentation (max. 500 chars)	The claimant has not proved a) which data pertaining to him have been processed, b) if his personal data, which form part of a file or are intended to form part of a file and c) what form of processing took place. Advertising mailing, which is not connected with other acts which refer to collection, processing and combination of data pertaining to personal or public life of a person, does not constitute either processing of personal data or infringement of the recipient's individual rights, i.e. an injury to his personality or his feelings
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	This judgment raises the question, if the Courts conceive and interpret the definitions (processing/ file) and the provisions (moral damage in case of unlawful processing and injury of personality/feelings) of the data protection law in the same way, in which the legislator and the DPA do.
Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Civil/Penal Law Supreme Court has overruled the action for cassation
Proposal of key words for data base	Direct marketing, Processing of personal data, moral damage

Case title	3833/2003
Decision date	Not available in the database
Reference details	Court of Appeal – Athens
Key facts of the case (max. 500 chars)	A company which provided financial information services (credit reporting) has collected, processed and transmitted to a commercial company data concerning the credibility/creditworthiness (unfavourable financial data) of the individual, who claimed the restitution of his moral damage, caused also by the fact that the commercial company, when refusing him to buy an air-conditioned by installments, has informed his wife for his financial situation
Main reasoning/ argumentation (max. 500 chars)	A company which provides financial information services (credit reporting) .has lawfully collected and processed data about the credibility of individuals, (consumer credit information) even without its consent. This Company has complied with its information duties through announcement in press, by which it has also informed about the categories of recipients of the data collected/processed. An interpretation of its duty to inform the data subject each time and in concreto in case of information being announced to third parties would exceed the purpose of these provisions. The commercial company failed to meet its information duties, as it should have informed the data subject for seeking information from the financial information company. By announcing his financial data to a third person (his wife) it has also committed the crime described in Art. 22 § 4 of the Law 2472/97 (unlawful disclosure of data)
Key issues (concepts, interpretations) clarified by the case (max. 500 chars)	The extent of information duties in case of disclosure/transmission of personal data to third parties depends upon the information provided to individuals about the categories of usual recipients of data. Seeking information about the creditworthiness of a data subject is subject to information duty.

Results (sanctions) and key consequences or implications of the case (max. 500 chars)	The Court of Appeal accepted that the data subject has suffered moral damage and awarded 5879 € as restitution for moral damage
Proposal of key words for data base	Financial services, credit reporting, credibility, Information duties, recipient, moral damage