Personal Data Protection

Coordinator **LDH** Ligue des droits de l'Homme

Partners **AEDH – EDRI – IURE - PANGEA**

GREECE NATIONAL REPORT

AEDH

This publication has been produced with the financial support of the Fundamental Rights &Citizenship program of the European Commission. The contents of this publication are the sole responsibility of LDH,EDRi,AEDH, Pangea, IuRe and can in no way be taken to reflect the views of the European Commission.

December 2009

TABLE OF CONTENTS

SYNTHESIS

Methodology

The principle objective of this study is to understand and learn from the current situation with regard to privacy and data protection in Greece. In particular, the aim is to explore practices, technologies and legislations that affect the everyday life of young people and finally to draw some conclusions.

The main questions asked were:

- How are European laws and EU policies relevant to data protection implemented in Greece?
- What are the main risks for data protection in Greece?
- How are young people affected by these risks?
- How aware are young people of these risks?
- What is the role of the Greek Data Protection Authority in eliminating these risks?
- What are the future challenges in this field?

This study is structured in 4 chapters: Mobility and Transport; Biological identity; Internet and telecommunications; Social Networks.
First, this work requires an excellent knowledge of EU developments in this area and a comprehensive research in reports and statistical reviews at the European level. In this context, documents issued by the European Data Protection Supervisor, the Article 29 Working party, as well as relevant studies of the Eurobarometer, were of significant importance for the study.
In order to determine the national situation, the observation method was largely used and a limited number of interviews were carried out. At the same time an extensive research in the case-law of the Hellenic Data Protection Authority (HDPA), other relevant independent authorities and the national courts was deemed essential.
Using the observation method, the research panned out to gather data from all possible sources which include books, related internet sites, NGO reports, online newspapers, periodicals, academic publications, government studies, independent studies, papers from seminars and other institutional publications, to give us the widest choice of perspective on the subject area.

The direct communication method was used to conduct a face-to-face interview with Philippos Mitletton, National Expert on Data Protection for the European Commission and a telephone interview with Vasilis Zorkadis, director of the Hellenic DPA. These two interviews were of great importance in order to identify the problematic areas in the Greek society and to provide us with some guidelines for the rest of the research.
The reason why most data refer to the Hellenic DPA is that - as it will be later on demonstrated - it is the main provider of information in this area. Most of the other sources were used to cross-check information, measure public awareness, determine public opinion and criticism.

Even though these sources have provided valuable information pertaining to data protection in Greece, it should however be noted that, as the AEDH worked on 3 countries and the EU, this study and the attached cards are not as thorough as those prepared by the partners working only on their own countries (France, Czech Republic and Spain).

Consequently, for the drafting of the cards priority was given to technologies and practices that have not been dealt with by other countries or that ascertain the main privacy concerns in the Greek society. In this context, the partners decided to include the card on video-surveillance, even though in the original plan CCTV was excluded from the scope of this project, since it is the most visible privacy-related phenomenon in the country. The card on the creation of a DNA database envisages to reflect the current developments in this field; the one on the pilot project at the Athens airport illustrates an

additional risk deriving from new technologies and enhanced control measures while at the same time it marks a case when the Hellenic DPA has been efficient and taken into account by the relevant actors; the card on the lie detector device, while not being a characteristic of the Greek society - since its use was very limited - demonstrates a new kind of risk for privacy and draws upon the problematic of overlapping of the two independent authorities; finally, the cards on the social networks were selected in order to analyse two websites that are not used (or not as much) by the other countries participating in the project.
This synthesis does not only aim to serve as a summary of the technologies and practices explained in the cards; it envisages to further cover issues of the Greek reality that fall within the scope of the 4 chapters agreed by the partners. This information includes the implementation of the EU legislation regarding for example, SIS, VIS, the Treaty of Prüm but also biometric passports, examples of use of CCTV in the private sector, spam and direct marketing etc.
Last, it should be noted that the research on Greece was concluded in late July 2009; therefore it does not refer to more recent developments (see also Note 22).

Legislation regarding privacy

There is a significant number of constitutional provisions pertaining to the rights of privacy and secrecy of communications. Article 9 states: "(1) 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. (2) Violators of the preceding provision shall be punished for violating the home's asylum and for abuse of power, and shall be liable for full damages to the sufferer, as specified by law."

A constitutional amendment in 2001 added a new provision to this article granting individuals a *direct right to protection of their personal information*. Article 9A, states: "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". It should be emphasized that *article 9A further establishes the Data Protection Authority***:** "The protection of personal data is ensured by an independent authority, which is established and operates as specified by law."
Article 19 of the Constitution protects the privacy of communications. The 2001 amendment, in addition to adding two new provisions to this article, establishes *an independent authority, to supervise matters relating to telecommunications*. Article 19(2) now states: "The matters relating to the establishment, operation and powers of the independent authority ensuring the secrecy of paragraph 1 shall be specified by law." Article 19(3) states: "The use of evidence acquired in violation of the present article and of articles 9 and 9A is prohibited Article 9A of the Greek Constitution".[1]

Greek data protection law was written to directly adopt the EU Data Protection Directive (95/46/EC). The Act was also necessary for Greece to join the Schengen Agreement. Greece has also incorporated into its national law all of the EU privacy protection Directives in the telecommunications sector, with the exception of the most recent Data Retention Directive.[2]

On the 6th December 2007 an amendment to Law 2472/1997 was submitted, which changes significantly its scope. The amendment introduces the following : (a) non implementation of data protection by the courts, prosecutors and monitor services (i.e. police) in the administration of justice and for the need of crime investigation concerning felonies or offences committed on intent and (b) the

[1] From http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559534
[2] Even though a Special Committee on the transposition into Greek law of Directive 2006/24/EC, where both the HDPA and the ADAE are represented, was established in February 2008, Greece has not yet transposed the data retention directive (consultation by government should be implemented by 15/3/09) and therefore the EU Commission has started a procedure of violation of Community Law against Greece.

declassification of prosecution and conviction as sensible data, for the processing of which normally the permission of the Authority is required.
In the above-mentioned cases, the provisions of common legislation apply and this means that the public prosecutors and other judicial authorities are not bound by the data protection, but only by criminal law provisions, such as the Penal Code and Penal Procedure Code. However, there are no concrete provisions for data protection in these acts or in other relevant legislation. This exemption is contrary to provisions of international treaties signed by Greece, such as Convention No. 108/1981 of the Council of Europe and Article 8 of ECHR. Most importantly, providing exemption in the above case is considered unconstitutional.

Moreover, this amendment allows to record audio and video during demonstrations, for the confirmation of serious misdemeanours and crimes after a prosecutor's instruction and if there is a serious imminent threat for public order or safety, in order to use them as evidence before courts.

In this case, the legislator, instead of perhaps incorporating some of the provisions of the directive issued by the Greek DPA on CCTV, introduces a legal provision that is in principle contrary to the constitutional right to freedom of assembly, since it can be argued that people knowing that they are being monitored feel fear and justified concern that might lead them to not even participate in peaceful demonstrations.

Recently, in July 2009 a new amendment has been announced by the Ministry of Interior, according to which the material collected from the operation of special technical devices for recording audio and video is exempted from the provisions of Law 2472/1997 on the protection of sensitive personal data. This means that CCTV could operate 24h/day and while the process of recording takes place under the supervision of prosecutorial and judicial authorities, there is neither a review by an independent authority nor the data protection act is applicable! As a result, there is a real need to give optimum attention to issue of video surveillance, which should be be subject to a separate article or even a special legislation.

Together with the amendment on CCTV, another amendment to the Greek law was discussed in the Parliament. This bill would result in the creation of a DNA database for offenders of most of the crimes of the Penal Code. It is obvious that the generalisation of collecting DNA material for a large number of offenses does not take into consideration privacy aspect and could implicate further risks.
In late June 2009 the Prosecutor of the Supreme Court has issued an opinion stating the following:
- Privacy of communications does not apply to internet communications and "external" elements of communication (names and other subscriber information, telephone numbers, time and place of call, duration of call, etc.).
- The prosecuting and investigating authorities, and in particularly the Judicial Council and the Courts are entitled to demand from the providers of communications services via the Internet the electronic traces of a criminal act, the dates and information of the person corresponding to the electronic record, and from other providers of communications services the "external" elements of communication ; the provider is obliged to deliver this information without the prior permission of an authority and especially the authority of ADAE[3].

- ADAE and any other independent body is not empowered or entitled to check in any way, directly or indirectly, whether the decision on the waiver of privacy of the institutions of justice is legitimate or not. This is judged by the judicial authorities only. Neither can this Authority control if the providers of communication services comply with the decisions of the institutions of justice. If it does so, it acts in excess of its jurisdiction.
According to this opinion communications via the Internet are not covered by the privilege of privacy as defined in Article 19 of the Constitution. This means that all sorts of authorities may have free

[3] Hellenic Authority for the Information and Communication Security and Privacy

access to the content of e-mails, chats, conversations via Skype, trades, etc., even to hard disks of computers.

It should also be noted that the Penal Code considers the breach of privacy a criminal act. Under the existing legislation companies are required to waive the confidentiality of communications only for certain very serious offenses. The abolition of privacy on the Internet is a global innovation and is contrary to all relevant provisions of the European Union. Furthermore, the European Court for Human Rights in the case Copland v. UK has decided that to surfing on the Internet itself, but also a list of e-mail sent by anyone, regardless of the content of web pages or messages, is covered by the protection of privacy. The European Court of Human Rights has therefore considered in 2007 that the "external data of communication" i.e. non-published information concerning the use of Internet is protected as part of individual privacy. So, national legislation providing guarantees for private communication should also be applied in the case of Internet.
In the light of this recent opinion a prosecution in degree of misdemeanour has been brought against 5 mobile phones companies, after their refusal to deliver specific data of owners of mobile phones and users of Internet services, which seem to have committed criminal offenses by phone and internet (offenses were misdemeanour acts, such as abusive messages).
Also, ADAE may be accused as an instigator of the above mentioned offenses as it has pointed to the telephone companies and companies providing Internet that the prosecutor's request infringes the law on personal data.

Privacy and Data protection Control Authorities

Hellenic Data Protection Authority

According to Art 15§2 of Law 2472/97 "*The Authority constitutes an independent public authority and will be assisted by its own Secretariat. The Authority shall not be subject to any administrative control. In the course of their duties the members of the Authority shall enjoy personal and functional independence. The Authority reports to the Minister of Justice and its seat is in Athens*". Its mission is the protection of the personal data and the privacy of individuals in Greece, in accordance with the provisions of Laws 2472/97 and 3471/2006. The primary goal of the HDPA[4] is 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).

Furthermore, another goal of the HDPA is to offer support and guidance to controllers in their effort to comply with their obligations vis-à-vis the Law, while taking into account the needs of the services in the Greek society, as well as the growing use of modern digital communications and networks. As a result of the above, the HDPA focuses, among others, on the identification and solution of problems which arise from the development of new technologies and their applications.

The HDPA has regulatory and consultative powers and competences such as licensing and registration, examination of complaints, imposing sanctions and implementation of international agreements (Schengen, Europol). It publishes an annual report and cooperates with international bodies such as, the Schengen Joint Supervisor Authority, the Europol Joint Supervisory Body, the Art. 29 Working Party on data protection, the Contact Network of Spam enforcement Authorities (CNSA), the International Working Group on Data Protection in Telecommunications (IWGDPT) and the Working Party on Police and Justice (WPPJ).

[4] Hellenic Data Protection Authority

The HDPA may impose administrative sanctions (art. 21), like warnings, fines, temporary or definitive permit revocation, destruction of files, locking of data etc. The law also provides penal sanctions (art. 22) and civil liability (art. 23).

A general comment about the sanctions imposed by the HDPA is that fines are more meaningful and effective when they target private companies/individuals. On the other hand, some fines imposed to the Ministry of Public Order are not effective and illustrate that the DPA cannot enforce its opinions. In general in 2008, the HDPA imposed 18 fines, 8 warnings and 3 other measures (destruction of data, destruction of records). It should be noted that the amount of fines imposed is significantly higher for private companies.
An illustrative case of the lack of political will to comply with the decisions of the HDPA is mentioned in the card on video surveillance.

In 2008 the HDPA issued 4 press releases. It has organised an event for the European Day for the Protection of Personal data and a seminar in Patras in November. Furthermore, some members of its staff have intervened in national and international seminars and published articles in the Greek press. The website of the Greek DPA is fully operational since December 2007. The most important documents issued by the Authority may also be found in English. Its website also contains a special column for kids explaining their rights, especially with regard to new technologies. Furthermore, citizens may file complaints, ask questions, apply for the list of article 13 etc, through the DPA's webpage.

According to a study on Citizens' perceptions on Data protection, published by the Eurobarometer in February 2008, 51% of Greeks are aware of the existence of the DPA, which is the highest rate in the EU. It is also remarkable that the awareness level has increased by 25% since 2003 when the last study was conducted. 5% of these persons have already contacted the DPA for a complaint or for information.

The HDPA is particularly interested in Passenger Name Records, Social Networks, Search engines/Search logs, Access to public documents, Marketing, Spam, Media, Industrial relations, CCTV and the Schengen Information System and the National List of undesirable aliens. The public may find information on these topics in the website of the HDPA. The Greek media is mostly interested in CCTV, biometric data, cybercrime, data protection in industrial relations, telecommunications and banking and regularly asks the Authority for information on the above mentioned subjects.

During the XIV Case Handling Workshop 2007 organised by the Greek Authority in November 2006, the protection of personal data of minors was raised for the first time. The Authority has so far received various appeals and complaints for violations of Law 2472/1997 which concern minors. In particularly, during the workshop it was underlined that there is need to deal with cases where there is processing of personal data of minors, due to their vulnerable and sensible character but also because of their particularity mainly because of lack of legal capacity, since minors can not give their consent for the processing of personal data, which is the rule for the legality of processing. Moreover, it was noted, that there are several domains where there is often illegal processing of personal data of minors, such as education, health, internet and marketing.
So far the HDPA has issued the following Regulatory actions (published in the Government Gazette of the Hellenic Republic):

- 408/1998: Informing the data subject by the press
- 1/1999: Informing the data subject (pursuant to the art. 11 of law 2472/97)
- Presidential Decree 79/2000 ratifying the regulation of the authority concerning frequently used categories of files and of processing for inclusion in special/simplified rules
- 24 and 25/2004: Data collection, maintenance and processing by TEIRESIAS S.A (interbank

system in order to minimize the risks involved while entering into credit contracts with uncreditworthy clients and, in general, to minimize the creation of doubtful debts, in the protection of commercial credit as well as in the improvement of economic transactions)

- 26/2004: Conditions for the lawful processing of personal data for purposes of advertising or direct marketing and the ascertainment of credibility,

and the following directives:

- Directive 523/18 on the conditions for lawful processing of personal data of new mothers for the purpose of direct marketing and advertising in the maternity clinics.
- Directive 1122/2000 on the closed circuit television
- Directive 1619/2000 on the application of Article 28 of the new Employee Code (Law 2683/1999)
- Directive 115/2001 on the processing of personal data in the field of industrial relations
- Directive 1/2003 (modification of the directive 1122/2000)
- Directive 2/2003 on the transcription in Roman characters of the name of individuals in identity cards and passports.
- Directive 1/2005 on the secure destruction of personal data after the end of the period that is required for the accomplishment of the processing purpose.

In 2008 the HDPA dealt with 859 cases, 263 of which were appeal/complaint cases and 596 questions. Number of decisions in 1999 (first year of operation of the DPA), 22, in 2006, 68, in 2007, 65 and in 2008 the number reached 69. In 2001 the highest number of decisions were taken, 163.

The total number of incoming documents in 2008 (appeals, questions, complaints, notification of keeping of records, applications for the list of art. 13, etc) was 6706. 818 of these were complaints/appeals, 216 of which on specific issues, in particularly 64 about CCTV, 4 about biometrics, 79 about spam and 69 about direct marketing. Only 55 complaint/appeal cases on the above mentioned issues were resolved (this number is general and does not necessarily include cases received in 2008) while there are still 516 pending cases. The number of questions received for these issues in 2008 was, 120 for CCTV, 16 for biometrics, 26 for spam and 34 for direct marketing. There are still 224 questions on these issues pending from previous years.
These numbers show us the serious difficulties facing the Greek DPA to cope with the rising number of cases and questions received, which becomes even heavier as pending cases from previous years accumulate.

Other authorities

Relevant authorities with the work of the HDPA are the Hellenic Authority for the Information and Communication Security and Privacy (ADAE), the Hellenic Telecommunications and Post Commission, the Greek National Council for Radio and Television, the Secretariat for the Protection of Consumers, the Greek Consumer Ombudsman and the Greek Ombudsman.

The Hellenic Authority for Communication Security and Privacy (ADAE) has been established under article 1 of the law 3115/2003, following the guidelines set in paragraph 2 of the article 19 of the Greek Constitution, in order to protect the secrecy of mailing, the free correspondence or communication in any possible way as well as the security of networks and information. According to the current legal framework ADAE is the most competent body to ensure confidentiality of communications, the concept of which includes elements of communication (traffic and location data) and it has issued some regulations concerning privacy in telecommunications to ensure privacy in mobile, fixed telecommunications services, through wireless networks and in internet communications and submitted various legislative proposals to the Greek parliament. ADAE is responsible to submit its decisions to the Minister of Justice. At the end of every year, all the activities performed and the actions taken by ADAE are submitted to the President of the Parliament, the Minister of Justice and the Greek parliament.

The shared responsibility between the HDPA and ADAE may result in multiplying opportunities for improving data protection but it may also be translated in weakening the protection as the authorities' concurrent powers seem to be lacking clear boundaries. So, the overlapping of competences of the two authorities could in practice also mean that there is a risk of division and decrease of control.

Privacy awareness

According to the aforementioned Eurobarometer study, 67% of Greeks are concerned about data privacy, (for the EU this number reaches 64%) and Greeks are the most likely to disagree that their personal data was properly protected in Greece (only 26% agree with this statement, while the average for the EU is 48%).
The 2008 annual report of the HDPA mentions that the Authority lacks means and personnel to develop its communication policy. Currently, the HDPA has 50 employees and according to its estimations it should have 150 staff members in order to be able to respond to the workload. The number of cases brought to the Authority rises every year, which together with the different activities that the staff has to participate, such as representation of the DPA in international bodies, participation in law-making committees, answer to parliamentary questions etc, leaves little time to deal with complaints and even less to organise awareness campaigns etc.

Most NGOs are only incidentally concerned with data protection; media exposure is restricted to law amendments and video-surveillance: some individuals are preoccupied with these issues and spread the word through blogging; however most of the debate in this field is going on in the academic field and in specialised publications (for example for lawyers).

One of the rare campaigns was initiated by the NGO ΔΗΜΟΚΡΑΤΙΚΗ ΣΥΣΠΕΙΡΩΣΗ, concerning the use of CCTV by public authorities. Another case that was the centre of public debate and where an important citizen movement was involved, concerns Greek identity cards. On May 4, 2000, in a controversial ruling, the DPA ruled that religious affiliations must be removed from state identity cards. The decision was opposed by the Greek Orthodox Church and led to massive protests and challenges to the ruling. The strong connection between the Greek Orthodox Church and the State is notable as there is no separation between Church and State. In March 2001, Greece's highest administrative court upheld the ruling finding that stating citizens' religious affiliation on the compulsory identity cards was unconstitutional. Prior to the ruling, Greece was the only member of the European Union that required citizens to list their religious beliefs on citizen identity cards. The new Greek identity cards do not include religion, even on a voluntary basis. In addition to the removal of religious affiliation, new identity cards also no longer include fingerprints, names and surnames of the cardholder's spouse, maiden names, professions, home addresses, or citizenship[56].
Lately there is a trend, mainly promoted by part of the press, to use hidden video products and phone-tapping as evidence of extortion or other punishable criminal acts. Therefore, media seem to encourage citizens to become improvised detectives in order to "reveal the truth". Thus, secret surveillance appears to be something obvious and normal, even if such activities constitute criminal acts punished according to the Greek Penal Code. This absurdity dissolves the core of human privacy while granting impunity.

Transport and mobility

[5] Source : Privacy International (http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559534)
[6] The DPA has also issued decisions about the stating of religion in school certificates (77A/2002), in public documents, such as birth certificates (134/2001) and about the stating of nationality in the identity cards (44/2001)

SIS, VIS, Eurodac

Greece ratified under Law 2514/1997 the Schengen Agreement, the Convention implementing the Schengen Agreement and the protocols and agreements for the accession to the Schengen Agreement of the other Member States of the European Union. Furthermore, in Article 82 of Law 3386/2005 for the entry, stay and social integration of third country nationals in the Hellenic territory it is provided that the Ministry of Public Order (now Ministry of Citizen's Protection[7]) maintains a list of undesirable aliens. The criteria and procedure for registration and removal of aliens from the list is established by a common Ministerial Decree (Minister of Interior, Public Administration and Decentralization, Foreign Affairs, Defence, Justice and Citizen's Protection).
The Data Protection Authority under Article 19 paragraph 1 and 114 of the Convention implementing the Schengen Agreement and article 19 of Law 2472/97 exercises independent control in the national part of the Schengen Information System (N-SIS). Its competence, therefore, includes the review of the legality of the entries in SIS taken by the Greek authorities. Based in Article 19 paragraph 1, the Authority is also responsible to verify the legitimacy of each file, and therefore the entries made in the National List for Undesirable Aliens. Persons who are registered and feel that there is any reason to delete them, may refer to the Authority. Therefore cases brought to the DPA concerning SIS are complaints aiming at deleting certain individuals from the SIS and the National List for Undesirable Aliens (for example because *the fact that the Greek nationality was withdrawn by the applicant can not in itself be a presumption of risk and therefore justify the inclusion of his/her name in the above mentioned lists*).

Transfer of data from SIS to third countries or international organisations is prohibited and if case be, the HDPA is competent to decide on this matter.

In decisions 5,6,7/2009 on complaints aiming at deleting certain individuals from the SIS and the National List for Undesirable Aliens it took the Authority 2 or 3 years to decide on the relevant cases. This practice obviously does not respect the deadline criterion (six-month delay) and is quite alarming as far as the efficiency of the DPA is concerned, since in reality it looses its value as an alternative dispute resolution mechanism.

In Greece the SIRENE Office[8] functions under the Directorate of International Police Cooperation of the Greek Police. Its responsibilities include communication with the respective offices of SIRENE in other Contracting States and coordination between national service providers which are competent, according to Article 94, for the registration of data into the system and for the services which are authorized to access to the system. In the SIRENE Office there have been mounted on secondment, under Article 21 paragraph 4 of Law 2521/97, two judges (a First Instance Court Prosecutor and First Instance Court President), to verify the legality of the entries in the National School of SIS. The presence of the judiciary intended to assist and participate in reviewing the legality of each registration is assessed as positive by the Authority, but their role should be strengthened. Possibly, the increase in the number of judicial officers would contribute to the effective operation of controls.

The Authority is regularly informed about the persons authorized to have access to the system. Public authorities authorized to feed the system are: the SIRENE office, the Directorate of Immigration of the Greek police, the Directorate of State Security and the Directorate of Public Security of the Greek police. Public authorities authorized to have access to the system are: The Ministry of Citizen's Protection, the Ministry of Foreign Affairs, through the Consulates, to control persons seeking a visa, the Ministry of Justice, the Ministry of Finance, through the Customs (on vehicles and weapons), and

[7] Former Ministry of Public Order
[8] For the function of communication and coordination of the National section of the Schengen Information System (N-SIS), there is a SIRENE Office operating in every Member State.

the Ministry of Merchant Marine, through the Coast Guard, to control ports and other entry points in the Schengen area through sea.

The Authority participates with two members and two alternate members to the Joint Supervisory Authority (JSA) for Schengen, which meet at the headquarters of the European Council in Brussels.
In reference with the operation of the SIRENE Office and the effectiveness of the National Section of SIS there have been major efforts to improve the security of the system and cooperation with the Supervisory Authority. However, some problems still exist as far as the operation of the competent office of the Directorate of Immigration, in particularly concerning the time of response to the documents of the Authority on the content of entries as well as the time required for compliance with the decisions of the Authority for cancellation of registrations that were deemed illegal.

During a visit to the Directorate's headquarters it was found by the HDPA that neither the people are enough to handle the responses nor the working conditions facilitate the effective operation of the service, which has serious consequences for the early fulfilment of the rights of interested persons. Also, in many cases, the information transmitted to the Authority is not complete in the sense that it either does not include all the requested information or does not contain sufficient justification of the reasons for the registration. Finally, the Authority considers that the competent authorities show great firmness regarding the registration of foreign citizens in the SIS. Cases of refusal to asylum applications, or simply illegal entry into the country, when not linked to criminal behaviour, should be weighted differently from cases of conviction, arrest or prosecution of criminal behaviour in general. The ease with which cases of the first class are being recorded has often resulted in conditions of inequality and social injustice.

The Greek data protection framework fully applies for the VIS and Eurodac systems so as for the data subject's rights to be effectuated. Furthermore, the HDPA has the necessary powers to deal with relevant cases. It also participates to the meetings of the EU DPAs organised by the EDPS concerning EURODAC supervision.

PNR

Greece does not have separate bilateral agreements with third countries, to exchange PNR-data. In 2003 Olympic Airways (OA) submitted a request to the HDPA, concerning PNR agreements with the US. The HDPA issued 2 decisions on the matter based on the directive and the agreement. According to the first one (4/2004) the Authority 1) may defer the decision on authorization for transfer of personal data to the U.S. and 2) decides to grant «OA» temporary permit for the transmission of personal data of passengers flying to the United States for a period of three (3) months under the following conditions: a) «OA» should fully inform passengers about the transmission of their data to the USA, before booking a flight to the USA and b) passengers should provide prior written consent for this purpose. The second decision (67/2004), in the light of the adoption of the PNR agreements at the EU level and taking into consideration the relevant opinion of the Group of article 29, gives to Olympic Airways the authorisation to transmit the personal data of passengers travelling to the US.
Furthermore, in its 2006 and 2007 annual reports the Greek DPA makes reference to the PNR and to the opinion 5/2007 adopted by the group on article 29: The general evaluation of the Group is that the level of protection of personal data has been considerably eliminated in comparison with the last agreement. In particularly:

- Even more data and data containing information about third persons can be transmitted according to the new agreement,
- The Bureau of Customs and Border Control of the U.S. can from now on in exceptional cases process even sensitive personal data,
- The duration of retention has been increased to 15 years

• The mechanism of control of the system of transmission does not involve independent authorities. Generally the safeguards provided in the new agreement are vaguely worded and thus leave open the possibility of many exceptions, which are at the discretion of the U.S.
Less than ¼ of Greeks seem to be aware of the transfer of their personal data beyond the borders of the EU. According to the study by the Eurobarometer on data protection, 22% of Greeks are aware of this situation (average in the EU 17%, highest rate in Luxembourg and Hungary with 33% awareness). Moreover, with regard to monitoring of peoples details when they fly with a view to combat terrorism, Greeks tend to believe that even suspects for terrorist activities should only be monitored under the supervision of a judge or equivalent safeguards.

European Biometric Passports

Under Law 3103/2003 the issuing of Greek passports is assigned exclusively to the Greek Police (EL.AS) from 1 January 2006. Under Law 3243/2004, those passports which were issued before the implementation of the new procedures, ceased to be valid from 31/12/2006. The current procedure results from the need to adapt the relevant EU regulation.
What elements does the Greek passport now include? Elements of the personal status of the holder, i.e. surname, name, nationality, date and place of birth, sex and height of the holder. The surname, name and place of birth appear also in roman characters. Also on the same page appear the issuing authority, the passport number, the dates of issue and expiration, and a specially printed photograph of the holder. Finally, it includes the signature of the holder, and a storage medium (micro chip) in which the photograph and personal information are stored.

From 28-6-2009 electronic passports are issued, where the second element of the biometric fingerprints is incorporated in accordance with the European Regulation 2252/2004, as amended by EC 444/2009. The new biometric passports include one digital fingerprint of the right and one of the left forefinger of the holder. All the existing passports remain valid until the date of their expiration. Without fingerprints are be issued the passports for children under 12 years, as fingerprints of children at these ages change as they grow older, while an exemption applies to those who are unable to give fingerprints, because of a disability.
The new Hellenic passport meets international standards as set out by International Civil Aviation Organisation (ICAO). It has new security features, including a chip, which should show if the passport is genuine or that it has been tampered with and the facial biometrics on the chip will help link the passport holder to the document. The data on the chip is supposed to protect against skimming and eavesdropping, through the use of advanced digital encryption techniques.

According to the Greek police the data on the chip is secure. It is protected through three layers of security*:*
- A digital signature to show the encoded data is genuine and which country has issued the passport.
- A protection against unauthorised readings (skimming) through Basic Access Control, a secure access protocol.
- The data is locked down using a Public Key Infrastructure (PKI), which provides protection against encoded data being changed. PKI is a digital encryption technology, which enables validation of the data as being genuine and shows any change, addition or deletion on the passport chip.[9]
The Greek DPA is competent to supervise the use of biometrics in passports .The level of security of the new passports has been criticised by the Greek media, especially the risk of skimming and of cloning of information. Michael Mavis, Head of the Subdivision of Security Control and Telecommunications Fraud of OTE (Greek telecommunications Company) and Vice President of the Greek operator for Prevention of Fraud in Telecommunications underlined the weakness to guarantee the security of personal data contained in the «biometric passports», speaking at a workshop on security of electronic communications held jointly by the Technical Chamber of Greece and the Athens

[9] From the site of the Greek police

Bar Association in the building of the Ministry of Transport. «The risk of leakage of confidential information or cloning is real» he said and added that «it is particularly important as far as the data of biometric passports are concerned»[10].

Treaty of Prüm

The Minister of Public Order, during the Council held in Brussels on 15th February 2007 announced the *in principio* accession of Greece to the Treaty of Prüm.
The Minister made the following remarks:
He acknowledged that there are constitutional problems with the application of Article 18, that Greece doesn't want sensitive personal data to be included in the mechanism of the Treaty PRUM, namely regarding the DNA database and the exchange of information should only include the general profile, i.e. the age and sex of the individual. It must be noted that Greece has no such records and therefore it will require domestic legislation. In another controversial article (14) mainly dealing with large political demonstrations and extension to sports events, to avoid the risk of breaches of public order. Greece will cover only convictions, not the vague legal concept of suspects for dangerous acts, terrorism, etc. For the legal framework in Greece, the abstract meaning of the act which creates a suspect is not legally acceptable. It suggests, moreover, the provisions relating to personal data in three main categories, i.e. DNA, fingerprints and numbers of vehicles to be kept in harmony with the provisions of national law relating to judicial guarantees. Lastly, Greece asked for two years to have the adjustment of national laws.
The Authority submitted the following observations on the Treaty of Prüm to the Ministry of Justice in December 2006[11]:
The accession or non-accession of Greece to this treaty has serious implications on the existing acquis on the protection of individuals from the processing of personal data. The treaty of Prüm introduces the Principle of availability which reflects a general trend to facilitate information exchange in the field of law enforcement. For this reason questions about data protection raised by the Treaty of Prüm should not be examined separately but in the light of efforts to create general rules for data protection in the third EU pillar. The Treaty of Prüm does not contain specific provisions on the purpose of the collection and the exchange of data (that is, if the data, and especially genetic data will be processed only for the investigation of serious crimes or will be also used for the investigation of any crime. The Treaty neither specifies the circle of persons concerned (if for example the treatment concerns persons suspected or convicted or other subjects as well, such as witnesses. Furthermore this Treaty n contradiction with the existing rules on data exchange applied to Schengen and Europol (which is the transmission of certain data under strict circumstances), applies the rule of preventive collection of various personal data (several of which may be sensitive), for disposal to any other competent authority of the Contracting States.
On the other hand, it is undoubtedly positive the fact that the Treaty contains a specific chapter on data protection. In addition it contains different legal requirements of data processing for each category, which is consistent with the principle of proportionality, a fundamental principle of data protection. Finally, the positive aspects of the Treaty include the obligation to record all traffic to search for information, which is held by the competent authorities both by the State requesting the information and by the State which provides them, as this arrangement facilitates the task of authorities responsible for checking the legality of the operation of this system of information exchange.
Furthermore the creation of new databases by the Treaty of Prüm is in itself dangerous for data protection. In particularly, the database concerning DNA is considered the most "dangerous". According to Greek Legislation, art. 200A of the Penal Code authorises the collection and processing for the investigation of some limited crimes and under strict conditions (see also relevant opinion of the Authority 15/2001). On the contrary, under the Treaty of Prüm, the collection of DNA records may

[10] From the newspaper PONTIKI
(http://www.topontiki.gr/Pontiki/index.php?option=com_content&task=view&id=748&Itemid=62)
[11] In its 2006 annual report we can find the Authority's opinion on the Treaty of Prum

include any kind of crime. The Authority stresses the difference between DNA samples and profiles and the fact that the first ones are very sensitive data which in no case can be considered necessary to combat crime.

Video Surveillance

The use of CCTV is the most important issue regarding data protection in Greece. There is no specific law regarding private sector, however, the operation of CCTV is regulated by the Directive 1122/2000 which was issued by the Authority, under Law 2472/1997. As far as law enforcement agencies are concerned, the Greek government since 2007 has proceeded in some amendments of the existing legal framework with a view to using street cameras in order to certify crimes committed during demonstrations; the first one took the competence from the DPA and gave it to the High Court Prosecutor[12] and the last amendment was announced in July 2009 and regards the complete exemption of CCTV from the data protection framework.[13]
The case of CCTV used by public authorities is analysed in the relevant card. In Greece an enhanced use of CCTV in the name of public security is reported. The example of operation of CCTV in the streets during student manifestations is highly illustrative of this matter. Authorities are allowed to take pictures during demonstrations while the current legal framework leaves almost no space for control by the HDPA. The principles of purpose and proportionality are rarely respected; as a result, there is a violation of the Greek constitution and of the relevant European legislation on data protection.
A brief description of the jurisprudence of the Authority on the use of CCTV in the private sector can be found here:

Banks – Companies issuing credit cards

In the case of banks, the Authority issued its Decision 40/2001, which allowed the maintenance of data by banks up to 45 days. Also, in individual cases it has allowed the extension of time for keeping data from closed-circuit systems from companies issuing credit cards up to 90 days with specific terms and conditions. These cases were examined at the request of the companies.

Hotels

Placing cameras at indoor and outdoor facilities is decided on a case by case basis. The Authority has issued its Decision 84/2002, which sets some general conditions on the installation of closed circuit television in hotels. In the checks made by the Authority spaces typically where camera placement is prohibited are the following:
Restaurants (Café / restaurant / bar) except for the Cash Desks, Exit staircases per floor (if cameras were installed at the entrances of the ground floor and garage), Staff rooms, External cameras taking picture of roads, houses, Pool area.

Hospitals – Psychiatric clinics

In general, the installation of cameras in indoor facilities of hospitals where they may be recording sensitive data, such as patient rooms, waiting areas are medical treatment, etc. is prohibited. Placing cameras in such places may be allowed only if deemed necessary to protect the lives of patients, such

[12] On the 6th December 2007 an amendment to the Law 2472/1997 was submitted, which changes significantly its scope. The proposed amendment introduces the following : (a) non implementation of data protection by the courts, prosecutors and monitor services (i.e. police) in the context of detection of crimes and misdemeanours committed by deception and (b) the declassification of prosecution and conviction as sensible data, for the processing of which normally the permission of the Authority is required. Moreover, it is proposed to be allowed to record audio and video during demonstrations, for the confirmation of serious misdemeanours and crimes after a prosecutor's instruction and if there is a serious imminent threat for public order or safety, in order to use them as evidence before courts.
[13] For more information on this topic and on the use of cameras see card on CCTV

as to specific sections of psychiatric clinics, where after the request of the controller and an inspection of the Authority a permit with specific conditions may be granted.

Shared housing facilities – Parking Spaces

The installation of closed circuit television in public areas of housing facilities is allowed only under the following conditions:
-After explicit and specific consent of every renter or a decision of the General Assembly of the building which clearly indicates the consent of tenants to install closed-circuit television.
-The cameras should not control access to the individual departments, to neighbouring houses, roads and pedestrian streets
-The current manager of the building is the controller and is obliged to inform subjects that the space is under video surveillance
-The image without sound recording is permitted if the control unit is located in a common area with controlled access and the data is kept 48 hours at most.
The installation of closed circuit in parking space is permitted only when the cameras focus solely on protecting the property and not in adjacent areas and there are signs that inform the subject about the filming.

Closed circuit television in the workplace

According to the Directive 115/2001 of the Authority the use of closed circuit television to monitor and control workers is prohibited.
During the XVI case handling workshop organised by the HDPA in 2006, the way in which closed circuit television is handled in relation to the protection of the European institutions was examined, while there was a discussion on closed circuit television at work, road network, hotels and psychiatric clinics and hospitals. In particular, the Hellenic Authority distributed the questionnaire for the latter issue. The answers to this questionnaire were discussed during the Workshop. Twenty Authorities replied to it, of which only four responded that they have relevant experience. Regarding the installation of closed circuit television in hotels, the Hellenic Authority, gave a brief presentation which gave rise to debate.

Recent developments

Recently the Mayor of Athens and the Minister of Interior announced during a press conference that they were in favour of video surveillance in playgrounds as a response to «incredible vandalism and odd behaviour». They called the Authority to approve their request, expressing the belief that the decision of the Authority should take into consideration that «the camera does not monitor children but protects them». The alternative solution would be to assign the surveillance of playgrounds to teams of the municipal police and to recruit unemployed for this purpose.[14]
Furthermore, the Authority took a decision concerning Google street view (Decision 11/5/2009) according to which the HDPA reserved the right to judge the lawfulness of the processing after the submission of additional evidence and has not allowed since then to start the collection of images.

Biological Identity

The Authority has issued a number of acts and decisions on the protection of personal data of employees from the use of biometric methods of control when entering a business facility or in general facilities of legal entities of private or public law.

[14] Newspaper Eleftherotypia

It has been decided that the introduction and use of biometrics constitutes a processing of personal data of workers, which is not necessary for the purposes of control of entry and exit to the premises / building and of arrival and departure, and is therefore illegal *whenever it does not respect the principle of proportionality*.
In particular, the Authority has already imposed with its 245/9 (from 20/03/2000) decision, the suspension of processing of personal data of municipality workers with the method of fingerprinting for the purpose of controlling the entry and exit from a municipal building, on the grounds that the method goes beyond the purpose of processing. The Authority held, moreover, that the breach is not waived by the consent of subjects and milder ways should be chosen to exercise control of the employer.

Also, the Authority has banned, with its decision 52/2003, the pilot biometric system used at Eleftherios Venizelos Airport, which aimed at collecting and processing fingerprints and iris of the eye to verify the identity of passengers. The biometric system sought to ensure that the passenger who checked in was the same as the person who actually boarded the airplane. While observing that such cases should be decided on a case-by-case basis, the DPA ruled that the collection and processing of iris and fingerprint data for verification of passenger identity was not permissible. The biometric data process was unlawful because the gathering of personal data exceeded its purpose. The DPA noted that passenger identity could be ascertained in a "milder way" by requiring passengers to show an identity card along with the airplane ticket.[15] As a result, this pilot project was stopped and no further attempts of this kind have been reported.
Moreover, with similar considerations, the Authority held in its decision 59/2005, that the processing of biometric data for the functioning of a pilot project is not legitimate and therefore it is not allowed to collect and process fingerprint data for access control of supporters and those accredited to sports facilities.
On the other hand, with its decision 9 / 2003, the Authority considered that the rights of workers are not violated (as enshrined in particular with Directive 115/2001) by installing a biometric system (elements of the geometry of the hand), for the sole purpose of controlling access to particularly «sensitive» - from a security of public transport point of view – Atticus Metro facilities.

In addition, with the decision 39/2004, the Authority has, under certain conditions, authorised the collection and processing of iris data only for workers who enter and offer their services at the Centre of operations of Athens International Airport, with a view to ensure access to this area, as it consists a key area of utmost security, and the smooth operation of which affects the smooth running of the whole airport.

At the request of the Minister of Justice and on the occasion of the draft law with a view to combating organized crime, the Authority issued an opinion (15/2001) involving the use of DNA for solving crimes. The Authority, noting the special nature of genetic material and its pervasiveness in the disclosure of many aspects of the personality of individuals as well as their private life, called for an exhaustive list of the offenses for the clarification of which there may be recourse to this measure and for the limitation of this measure to particularly severe offenses. Alongside, it claimed the subsidiarity of this measure, namely its use only when there is sufficient evidence of guilt or involvement of some persons in a certain criminal action. According to the opinion, the genetic analysis of DNA must be limited to the "non-codified section of DNA" and identity verification .The HDPA advised that any methods that allow any conclusions about the personality traits of individuals from their DNA should be forbidden, including personality profiling. This method of investigation should only be used for verification of offenders' and victims' identity and for criminal investigations and should be destroyed once the fulfilment of the intended aim is achieved. Finally, the DPA does not support any effort to collect and analyze genetic material for preventative purposes.

[15] More information in the relevant Annex

The legislature, following the basic instructions of the Authority, with Article 5 of Law 2728/2001, has enabled the DNA analysis for the identification of the offender of crimes with the use of violence or crimes against sexual liberty or acts of membership or establishment of organisation according to Article 187 of the Criminal Code.
In July 2009, together with the amendment regarding CCTV, the government has also announced the creation of a DNA database where genetic data of people arrested for involvement not only in serious crimes but also in misdemeanours will be recorded. The genetic material for the DNA database will be collected obligatorily, following a court decision for everyone who brings a strong evidence of guilt, even for misdemeanour acts which result in three months prison sentence, leaving therefore outside this framework hardly any offenses mentioned the whole the Penal Code. Until now, Article 200A of the Code of Criminal Procedure provided that genetic material could be collected under the authority of the Judicial Council and only for serious crimes.

If the analysis of the DNA is negative, the genetic material and the genetic fingerprints are destroyed immediately, while in case the analysis is positive, the genetic material is destroyed immediately, but the genetic fingerprints will be retained in a special file until the death of the person concerned and will be used in investigating and solving other crimes. The archive of genetic material will be stored in the Directorate of Criminal Investigation of the Greek Police Headquarters. The file operation is supervised by the Appeals prosecutor or deputy public prosecutor appointed by decision of the Supreme Judicial Council, for a period of two years.

Interpersonal communications

In early 2006 it was made public that the mobile phones of a number of ministers and politicians (including the Prime Minister) were tapped for a period starting from the Olympic Games of 2004 until March 2005. Altogether more than 100 mobile phones were tapped, all numbers operated by Vodafone Greece, using Ericsson's software (the same companies first revealed the case, when "they were made aware of it"). The antennas through which the above mobile phones were tapped were all located in the area around the American Embassy in Athens, but no connection to it was established. The case held tremendous publicity, allegedly led to top-level management changes in the companies implicated, and also led to enactment of the Hellenic Authority for the Information and Communication Security and Privacy who led the relevant investigations. A Parliamentary Special Committee was also established, but none of the investigations or state initiatives led to any tangible results. However, the DPA fined Vodaphone 76 million EUR for failing to protect the network from the unknown hackers.[16]

In July 2008, Law 3674/08 was voted on strengthening the institutional framework to safeguard privacy of telephone communications. However, as mentioned in the chapter concerning legislation, an important restriction of data protection and of the control by independent authorities has taken place in the field of telecommunications as well.

According to the study of the Eurobarometer on data protection, only 6% of Greeks believe that their data is sufficiently secure in the Internet. This is the lowest rate in Europe. Furthermore, 63% believe that legislation cannot offer protection for data privacy in Greece. The study i2010 for the year 2008, by the Greek Information Society Observatory reveals that 95% of people between 16-25 years old use a PC, out of which 72% use it on a daily basis. 49% of those people send messages in chat sites or participate in forums. According to the 8th semester report on broadband in Greece, by the Greek Information Society Observatory, 70% of teenagers and 67% of persons between the age of 18-24 use internet.

[16] From http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559534

Lately there is a public debate about a legislation according to which the acquisition of card mobile phones would require the submission of identity data of the person to the company-provider, which would clearly change the current situation. Today there is an option: if someone wants anonymity has the option to buy card mobile rather than sign a contract with a telecommunication company.

The card on private communications is a case of a technology called 'layer voice analysis' used for commercial reasons. This technology was used by a telephone service offering to the users the possibility to know whether their interlocutor was telling the truth. However, the processing of the person's voice was taking place without his/her consent. This technology which immediately destroyed the file, only operated for 2 months. This case raises concerns about the use of new technologies and the protection of privacy of individuals and further opens the debate about the concurrent powers between the HDPA and ADAE.

Data retention (Directive 2006/24/EC)

Before the adoption of this Directive, ADAE, with its No. 54/24.8.05 decision, expressed the view that «any further restriction of individual rights of privacy of communication, designed to prosecute the crime and counter terrorism should be adopted only when it consists necessary, appropriate and proportionate measure within a democratic society and under the condition that it does not affect the core of constitutionally guaranteed individual right to privacy of communication». According to the HDPA, the Directive has as a result the restriction of individual rights, particularly the protection of personal data and confidentiality of communications, as enshrined in Article 8 of the European Convention of Human Rights (ECHR) and Articles 9 and 19 of the Greek Constitution. Therefore, a strict interpretation of these provisions so as to respect the principle of necessity and proportionality is required.

The HDPA and ADAE were asked by the Ministry of Justice to participate in a meeting in October 2006 with the aim to exchange views among stakeholders, including service providers. In preparation for the meeting, the Ministry of Justice sent a series of questions / issues and announced that it will establish a special committee for the processing of national provisions transposing the Directive.

Even though a Special Committee on the transposition into Greek law of Directive 2006/24/EC, where both Authorities are represented, was established in February 2008, Greece has not yet transposed the data retention directive (consultation by government should be implemented by 15/3/09) and therefore the EU Commission has started a procedure of violation of Community Law against Greece.

On the implementation of Directive 2006/24/EC of the European Parliament and Council for the maintenance of electronic data communications, ADAE in 2008 agreement participated in the meetings of the European Telecommunications Standards Institute (ETSI) for data retention.

Direct marketing

Direct marketing, is considered legal as it is a necessary component of the free market economy, but is subject to strict conditions laid down by the regulation 26/2004 on the Conditions for the lawful processing of personal data for purposes of advertising or direct marketing and the ascertainment of credibility and decisions of the Data Protection Authority. In particular:

If the advertisement is using electronic means (i.e. by phone, e-mail, SMS – MMS), then the Law 3471/2006 on the protection of personal privacy in electronic communications, sets strict conditions for carrying out any electronic communication with advertising view, therefore for a company to communicate with you it should have received your consent.

Anyone who does not want to receive promotional material, can make a statement for registration under Article 13 (Law 2472/1997) which is maintained by the Data Protection Authority and should be advised by the advertisers in order not to disturb those who do not want to receive advertisement. But, Law 3471/2006 on the protection of personal data in electronic communications, provides, that with the exception of e-mail that a company has received due to prior commercial communication, it is not permitted to use personal data without special prior consent of the subject.

If someone, even though registered, continues to receive advertising has the right to complaint to the Authority (which will impose a fine to the company), and also the right to damages in an action brought in the courts. The law also states that the minimum compensation amount is 6000 euro. In 2 cases of such injunctions, the courts of Athens awarded this compensation to persons who although they were registered, received promotional material to address them.

But even if someone is not written in the register, if he/she can prove that a company has not fulfilled the conditions for the legality of direct marketing, they can claim compensation. One of the most important reasons is the obligation to prior notice for the use of personal data of individuals, or if the advertisement concerns more than 1,000 people the obligation to notice through the press.
In the case of marketing of personal data for professional reasons, companies should issue rules for the processing of personal data, which must have the approval of the Authority.
The Authority has also issued Directive 523/18 on the conditions for lawful processing of personal data of new mothers for the purpose of direct marketing and advertising in the maternity clinics.

Spam

Since 2004 the HDPA created a working group with representatives of key public and private Greek internet service providers that identify the common desire to reduce the spam and discussed the adoption of a code of conduct for providers in order to combat spam. The code is not yet adopted as there was no consensus among team members on the integration of technical measures against spam. The HDPA is considering issuing directives/recommendations to the internet service providers in four areas: a) general policy reviews and information of clients, b) measures against outgoing spam, c) measures against incoming spam and d) measures for cooperation between Internet service providers.
In 2007 the Authority took part in the meeting of the CNSA (contact network for anti spam authorities). In the context of this collaboration, a representative of the German association ‘eco’ on internet service providers was invited to Greece to present the program spotspam which aims at creating a central database between competent European actors to combat this phenomenon. The HDPA signed a memorandum of collaboration with ‘eco’. Furthermore in the website of the Authority there is a special information space for spam. The authority also decided to issue guidelines-recommendations for internet service providers and electronic mail providers on the fight against spam in cooperation with ENISA. For this purpose on 20-5-2008, a meeting with representatives of providers, and of ENISA was held. According to its 2008 annual report, the Authority plans to publish a relevant act in 2009.
As an example of the Authority’s jurisprudence, the DPA adopted the decision 69/2008 imposing a fine to a company that sent mass SMS messages. The company for a long time was sending SMS asking the recipients to call a number of additional debt in order to receive products that they had won after draw. It was found that these messages were sent without prior consent of the recipients and without ensuring the rights of information and access. The Authority held that SMS were considered as e-mail, according to the definitions of Law 3471/2006 and Directive 2002/58/EC, that the numbers of mobile telephones are personal data and that it has the power to decide on compliance with Article 11 of Law 3471/2006.

Phone marketing

Decision 57/2007 deals in particularly with phone marketing stating that phone marketing should respect the same rules applied to spam, in particularly:
- The advertising company not only has to consult the register of Article 13, but it must also have the special consent of the subject.
- When the company uses independent "business partners" who make the calls, but determines the ways and purposes of processing, the advertised company remains responsible. This means that the advertiser can not abdicate its responsibility and pass it entirely on trading partners.

Others types of Direct Marketing

If the advertising is done through other, non-electronic ways (such as through paper correspondence) companies may send promotional material provided they can find the contact details from a publicly accessible source (such as telephone directories indicating addresses). In this case the company should inform the subject on how they found its information and give the opportunity to object to future promotions from it.

Search Engines

The website of the Greek Authority contains a special column on information about data protection and search engines, making reference to the potential dangers of search logs and providing links to relevant documents.
Furthermore, the Working group of article 29 adopted in April 2008 an opinion on the protection of personal data related to search engines, in the formulation of which the Greek Authority was involved. A key conclusion from the above opinion is that the Directive on the protection of personal data (95/46/EC) applies, even when the processing of personal data is done by search engines based in countries outside the European Union (as the major U.S. search engines Google, Yahoo!, etc.). Instead, the Directive on data retention (2006/24/EC) does not apply in the case of search engine providers.
In Greece, there has never been a Greek search engine that distinguished from the others and even the most popular ones like anazitisis.gr (Otenet) and find.in.gr (In.gr) were practically gradually not in use as they showed results from Google. Nowadays the only greek search engine is trinity.gr, by Phaistos Networks (Pathfinder.gr)

Social networking sites (SNS)

Facebook is the most popular social network in Greece. According to the data collected by insidefacebook.com. Greece ranked 25th in the total number of users of Facebook in August 2008. Currently (July 2009) there are 611,604 people registered in Greece network (information provided by facebook.com). According to Alexa.com[17], Facebook is the 2nd most popular website in Greece. hi5 ranks 23rd in the same list, and Myspace 20th. According to a study by Synovate on Youth Marketing and Best brands for young people in Greece (published in Adbusiness no.63), Facebook is the 2nd most popular internet brand for young people in Greece, Zoo.gr is the 6th and hi5 the 7th.

[17] Alexa is a website-usage information website, belonging to Alexa Internet Inc. a subsidiary company of Amazon.com. Alexa ranks sites based on tracking information of users of its Alexa Toolbar for Internet Explorer and from integrated sidebars in Mozilla and Netscape. Once installed, the toolbar collects data on browsing behaviour which is transmitted to the website where it is stored and analyzed and is the basis for the company's web traffic reporting. There is some controversy over how representative Alexa's user base is of typical Internet behaviour. If Alexa's user base is a fair statistical sample of the Internet user population (*e.g.*, a random sample of sufficient size), Alexa's ranking should be quite accurate.

Another study[18] reveals that 81,1% of people who use SNS and update their profiles at least once a month have a profile on Facebook, 23;9% use hi5, 15;1% Myspace, 9,7% Youtube and 3,5% Zoo.gr. Out of those having an account on Facebook, 61,3% use it daily. The great majority of people using SNS (82,8%) have in their profiles photos and about 50% have music and video and friends' announcements and comments. The main reasons for using SNS is to send messages to friends (82,2%), upload photos (51,8%), search for friends (50,6%), visit friends' profiles (48,4%) and send instant messages (45%).

According to the same study 88,2% of the people interviewed use social media such as blogs, SNS, file-sharing, forums, RSS readers, podcasts etc.
Zoo.gr is a popular Greek social network serving as a meeting and gaming point for its users. Most of its members join the website to play games such as backgammon and chess and to share photos and videos. Zoo.gr has made a notification to the HDPA concerning the processing of data of its users. The consent of the user offers the explicit consent of the subject for the processing and transmission of the subject's personal data. The registration to the site's newsletter and to advertising programs is optional. Moreover, the user can configure the browser in such a way that it either warns him/her of the use of cookies on specific services of Zoo.gr, or prohibits the use of cookies. Zoo.gr is legally bound not to sell or publish the data submitted by its members. So far, there were no complaints of unlawful use of data by this social network brought before the HDPA or the Greek courts.

According to Google trends[19], until the end of 2006, Hi5 ranked among the most popular networks in Greece together with myspace and zoo.gr. It gained a big rise in 2007 but as from summer 2008 facebook is by far the most popular social network in Greece. There have been reported phising emails posing as invitations to the website[20] and unsolicited bulk mail. In accordance with the rules of Hi5, any content posted by the members of Hi5, gives to the site automatically the right and "irrevocable, perpetual, non-exclusive, royalty-free and fully paid, worldwide license to reproduce, distribute, publicly display and perform (including by means of a digital audio transmission), and otherwise use Content and to prepare derivative works of, or incorporate into other works, such Content, and to grant and authorize sublicenses of the foregoing." Hi5 further shares the information posted in its website with third parties like advertisers. Publicly posted content can be viewed even by non-members of Hi5 who are visitors to the website. There is a potential high risk for young users of Hi5 who are not aware of the risks involved in the processing of their personal data by this social network.

In the beginning of June 2009 the Single Court of Thessaloniki issued the first decision[21] in Greece about personal data in Facebook, officially opening this debate. The case is a request for provisional measures submitted by a member of the teaching staff of the University against another candidate for the same position (of teaching staff) who posted documents about her studies and career development on a profile in Facebook, commenting them negatively. In fact, the candidate created a fake profile on Facebook where he published these documents accusing her she had relations with politicians, questioning her titles etc. These texts were sent to 300 people, academics, journalists and politicians. The court alleged that although the information was posted under pseudonyms, behind the act was the candidate, because he was the only person who had received the copies at the controversial time (by the applicant). It should be noted that these posts could be accessed by anyone (it was not a «closed» profile).

[18] Study on social media by the institute of communication operated by the MRB Hellas SA and published on the 18th February 2009
[19] Google Trends is a public web facility of Google Inc., about Google Search, that shows how often a particular search-term is entered relative to the total search-volume across various regions of the world.
[20] http://securitylabs.websense.com/content/Alerts/3205.aspx
[21] Decision 16790/2009

It seems that the Greek court took into consideration the decision of the European Court of Justice according to which personal data posted in publicly accessible websites is an act of «processing» of these. The decision demonstrated that even without a waiver of confidentiality, legal protection of personal data may be given by the Greek courts. The court held that this is an attack on the personality; it is an illegal act and imposed a penalty of € 1,000 for each infringement (publication and other such items). It should be finally noted that the applicant has made a complaint before the Data Protection Authority since last December which so far has not dealt with the case.
Also in mid-June 2009 a 22 year-old university student living in Crete (Chania) was arrested by the police because he had created an open profile in Facebook using the name of his landlady and posting her photographs without her consent. The student was let free until the trial for violation of privacy and defamation.
In March 2008, the International Working Group on Data Protection in Telecommunications (IWGDPT) published a document with recommendations for social network services. In the formulation of this document the Greek DPA participated actively[22].
The Greek DPA also offers information on social networking in its website. This column consists in a kind of warning for social network users, with links to important documents. The part of the website addressed to children is more general and talks about general dangers for privacy resulting from the Internet.

Conclusions and recommendations

It seems that data protection in Greece is at a critical point due to the lately adopted measures. Furthermore, since the government and the national authorities seem not to take into consideration the work and the opinion of the independent authorities[23], it is crucial to invest in a communication policy in order to contribute to the development of a data protection culture in the society.
Therefore, beyond the legal framework and the statutory powers, there is also a social role of the HDPA and ADAE. Raising awareness requires organization of seminars and campaigns, contacting representatives of political or social institutions, media-friendly attitude, use of new technology, communication with the youth, the elderly, the disabled and the aliens. Furthermore, they should have the means to develop a preventive action through the publication of studies, codes of conduct and through the issuing of new directives.
In this perspective it would be a good idea to translate, if possible, this comic book in Greek.
Moreover some conclusions could be made regarding the technologies described in the cards. In particular:

- Measures aiming at enhancing security (like the use of CCTV, or the identification of passengers through biometrical means) that pose restrictions to privacy should always respect the principles of purpose and of proportionality and the use of alternative milder measures should first be exhausted.
- The creation of a DNA database includes the risk of receiving DNA material for almost any offense, even for misdemeanours. However, DNA samples should be restricted to serious crimes only and to those offences who make necessary the taking of genetic material to find the perpetrator.
- Awareness among young people about the potential risks from the use of social networks and the available “techniques” to better “shield” their personal profiles should be strengthened.
- The competences of the independent authorities should be clearly defined in order to avoid overlapping and weakening of control

[22] Report and Guidance on Privacy in Social Network Services- ”Rome Memorandum” -43rd meeting, 3-4 March 2008, Rome (Italy)
[23] These conclusions refer to the situation before the national elections of 4 October 2009. Even if we do not have enough facts concerning the attitude of the public authorities towards "data protection", there are some vague indicators that the new administration counts a lot on civil society and, accordingly, on the role of the independent authorities, which may have a positive impact on data protection and privacy.

In general, one can observe that in Greece the surveillance society is increasing; biometrics, CCTV and telecommunications are widely used to combat crime and terrorism and social networks create new risks for privacy. The current legal framework limits the control by the independent authorities, in particular with regard law enforcement bodies and there is an urgent need to better involve civil society and promote education and awareness on these issues.

1-MOBILITY AND TRANSPORTATION

CCTV

Technology used/tool (For each teams, a card pro tool)	**CCTV**	
Country/ use area	Greece	
Frame of use	The Closed Circuit of TV is the basis of the function of Subsystem 17 of C4I. Subsystem 17 is a circulation surveillance system on the Roads of Attica. The system is being monitored and controlled by the Operations Room for the Monitoring and Control of Traffic of the Traffic Police Headquarters of Attica and is also available in distant Administration Centers (General Staff, Ministry of Public Order etc.). The elements that make up Subsystem 17, give the Operations Room for the Monitoring and Control of Traffic operators the possibility of access to video and sound from each one of 293 positions, wherever CCTV equipment is set up, as also to video from 49 cameras of the Hellenic Police. Each one of the 293 positions contains a pole 12 or 8 meters high with camera PTZ, sound box and microphone. Near each pole, an electric board contains the functional equipment of the system (codifiers, network transmitters, UPS etc.) and the Intelligent Traffic System (ITS) (in 282 positions).	
Population concerned: target and age	This measure concerns the total of the Greek population but in particularly young people, as they often participate in manifestations, demonstrations (see below known or potential risks)	
Trends (measured / supposed)	A more and more general and uncontrolled use of CCTV that does not respect the principle of proportionality and does not take into consideration the ruling of the Greek DPA.	
Known or potentials dangers / Risks	Operation of the system for purposes other than that of regulating the traffic of vehicles. In particular: According to Decision 58/2005 of the DPA “as to the primary purpose, that is, the traffic management, the operation of the system fulfils the conditions of proportionality	

	required by the law and only under certain conditions ensuring that the system is not used for any other purpose or by services of the Hellenic Police, other than those that have been legally entrusted with the management of the circulation of vehicles". The Authority imposed a sanction (fine of 3000 euros) to the Greek Police because it didn't comply with its provisions according to which "the operation of cameras installed on low traffic roads, squares, parks, pedestrian zones and citizens' assembly places (i.e. theater entrances) is forbidden and those cameras need to be removed" and "the operation of cameras installed on crossroads or road axes, when the traffic flow of vehicles is interrupted on them, i.e.during manifestations, demonstrations etc, is prohibited".	
Others		
Generated data bases		
Associated data base/ creation (a line per database)	With the decisions 28/2004 and 63/2004 the DPA had permitted the operation of the CCTV system which had been used for the security of the Olympic Games, for a specific period of time and under specific conditions (only for traffic management). With the request of the Ministry of Public Order-Hellenic Police Headquarters-Olympic Games Security Division (GPHA)it was asked to extend the time period of the operation of the closed circuit television system that is used for the purpose of traffic control, as specified in the decision No. 63/2004 of the Authority that expired on 18-5-2005.	
Data retention duration/ Right to be forgotten	The database and the equipment supporting the processing are kept at the Traffic Control and Monitoring Operations Room of the Division of Road Traffic Police. The data is kept for seven days, after the passage of which they will cease to exist.	
What justifies the inscription in the file /Risks?	Traffic management and protection of individuals and goods. Broad interpretation, risk for fundamental freedoms of citizens (see above known or potential risks)	
File masters? Risks?	Controller of the data will be the Ministry of Public Order/Hellenic Police and particularly the several services for which it has been asked to directly receive and process visual images.	
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Access to the data will have the official services of the Hellenic Police (GPHA, Traffic Police	

	Headquarters of Attica, Flying Squad Headquarters etc.).	
Right to know or to modify data? (appeal)	No information found	
Covert purposes/ Risks/uncontrolled future evolution	As we have already seen, CCTV is used for non-legitimate reasons. During the manifestations and the march on 17-11-2007, the anniversary of the resistance of students at the Polytechnic, there were pictures taken, in contradiction to the decision of the DPA. This led the President and other members of the Board of the Greek DPA to resign because they considered that this behaviour affected the independency and the validity of the Authority[24]. The DPA nowadays continues to issue relative decisions, but the national authorities do not seem to take it seriously. In general there is a tendency to increase the use of videosurveillance and to minimise the DPA control on CCTV (see below legislative amendments)	
Others (inter-connexions, …)		
Legislation in application		
Law /rules / trends, (if implemented for this data base or this technology)	Existing legislation but in practice not respected by the Greek authorities. -Article 8 of the European Treaty on Human Rights for the protection of private life. -Convention 108/1981 of the Council of Europe for the protection of Individuals with regard to Automatic Processing of Personal Data. -Articles 7 (protection of private life) and 8 (protection of personal data) of the Charter of Fundamental Rights of the European Union. -Directive 95/46/EC of 24 October 1995 for the protection of natural persons with regard to the processing of personal data and also for the free circulation of these data. -Articles 9 and 9A of the Constitution. -L. 2472/97 on the protection of individuals with regard to the processing of personal data. -Directive 1122/2000 adopted by the Greek DPA on CCTV	
Conformity with the European right (European charter of fundamental rights - directives…)	The recent amendments (see below) and the use of CCTV in practice is in contradiction with European law regarding the protection of privacy and the processing of personal data of	

[24] Press release published in Brussels in 6.12.2007 *"Data protection in Greece: The Art. 29 Working Party is deeply concerned about the development taking place in Greece after the resignation of the President and 5 members of the Hellenic Data Protection Authority. The EU Data Protection Commissioners stressed the importance of an independent supervision as foreseen by Directive 95/46/EC. The current situation has immediately to be remedied with a view to re-estabishing a functioning independent Data Protection Authority in Greece.*

	individuals. Also in contradiction with the case law of the EctHR (see for ex. Peck v. UK)	
Risks for freedoms despite the law	Violation of the right of privacy of citizens. According to opinion 4/2004 of the Working Party of article 29, according to which "the over-proliferation of image acquisition systems in public and private areas should not result in placing unjustified restrictions on citizens' rights and fundamental freedoms; otherwise, citizens might be actually compelled to undergo disproportionate data collection procedures which would make them massively identifiable in a number of public and private places."	
If revision of the regulation: for which reasons? Results: improvement or aggravation (compared to the protection of the DP)	In December 2007 an amendment of the data protection law, defined the High Court Prosecutor as the only competent authority to decide on the use of CCTV, thus totally ignoring the DPA[25]. Today the situation still continues and images are taken during demonstrations with the excuse of preventing and repressing possible criminal or terrorist acts. The authority has issued a more recent decision imposing a fine to the Ministry for violation of its decision 58/2005 (Decision 7/2008) In July 2009 a new amendment has been announced by the Ministry of Interior according to which the material collected from the operation of special technical devices for recording audio and video is *exempted* from the provisions of Law 2472/1997 on the protection of sensitive personal data. This means that CCTV could operate 24h/day. This material, if used in order to certify crimes committed during demonstrations, will be retained for as long as deemed necessary by the prosecutors. Alternatively, it will be kept 7 days in the archives of the Police and then destroyed by an act of the Prosecutor.	
Others		
This tools and young public or young adults		
How far are young people concerned?	Young people are particularly concerned, as it is usually them who participate in	

[25] On the 6th December 2007 an amendment to the Law 2472/1997 was submitted, which changes significantly its scope. The proposed amendment introduces the following : **(a)** non implementation of data protection by the courts, prosecutors and monitor services (ie police) in the context of detection of crimes and misdemeanors committed by deception and **(b)** the declassification of prosecution and conviction as sensible data, for the processing of which normally the permission of the Authority is required. Moreover, it is proposed to be allowed to record audio and video during demonstrations, for the confirmation of serious misdemeanors and crimes after a prosecutor's instruction and if there is a serious imminent threat for public order or safety**,** in order to use them as evidence before courts.

	demonstrations	
Awareness of issues or of risks / Indifference or reaction	Due to the mediatisation of this measure, the Greek public is highly aware of this practice and at least of some the potential risks related to it. According to a study by the Eurobarometer concerning Citizens perceptions of data protection in the EU, 37% of Greeks do not trust the use of personal information by the police. This study did not include a question concerning video surveillance, but with regard to measures used for the fight against terrorism, such as monitoring of phone calls, internet usage etc, Greek respondents were especially favourable towards a very restricted monitoring of their personal data. There are quite a lot of cases of attempts to break the cameras during manifestations, but as the law has been amended, there is not enough room for legal reaction.. However, the Greek DPA has issued an opinion (1/2009) on the last amendment regarding the use of CCTV in July 2007. According to this advisory opinion 1) the use of CCTV in public spaces is exempted from the implementation of Law 2472/97 and the competence of the DPA, 2) specification of the purpose of processing is required, 3)no specific criteria for 'dangerosity' are foreseen in order to decide whether the use of CCTV exceeds is a restriction necessary according to the ECtHR and the Council of State, 4)no effective protection of individuals is provided, 5)the controllers are not clearly defined, 6) the issuing of an administrative decision that would allow an effective judicial review is not foreseen, 7)there are non provisions on the collection, storage, use and transfer of data, 8) the DPA is no longer competent to supervise the use of CCTV which violates art.9 of the Greek Constitution and art.8 of the ECHR.	
Awareness campaigns/ results	A big campaign was organised to oppose to the use of CCTV by public authorities, by the NGO ΔΗΜΟΚΡΑΤΙΚΗ ΣΥΣΠΕΙΡΩΣΗ in 2006 and 2007 and it criticised the Decision 58/2005 by which the Authority gave permit to public authorities to use cameras after the Olympic games.	
Good practises	Not applied	
Campaign to be lead? On which themes	There should be a generated campaign on data protection rights with regard to the use of	

	CCTV in particular. This should also focus on the private sector (see below) where video surveillance is largely used as a panacea in terms of security or controlling, for example, employees. Greek citizens should realise that CCTV is not always the appropriate measure to fight crime and increase security and that risks to privacy should always be taken into consideration.	
Others	CCTV is used widely in Greece in the private sector as well (i.e. in banks, hotels, hospitals, shared housing facilities and the workplace) During the XVI case handling workshop organised by the HDPA in 2006, the way in which closed circuit television is handled in relation to the protection of the European institutions was examined, while there was a discussion on closed circuit television at work, road network, hotels and psychiatric clinics and hospitals.. This all shows that there is an alarmingly increasing use of CCTV in Greece	
Conclusions	The activation of cameras and the C4I system is a direct violation of Articles 11, 9 and 9A of the Constitution, and violates the right to privacy the right to demonstration and to peaceful assembly.	
Recommendations	Launch a large awareness campaign, change of political scenery to facilitate the protection of citizen's fundamental freedoms, competence of the DPA on the matter.	

2-BIOLOGICAL IDENTITY

PILOT PROJECT IN ATHENS AIRPORT

Technology used/tool (For each teams, a card pro tool)	**Processing of iris and fingerprint data**	
Country/ use area	Greece	
Frame of use	This pilot project was applied in Athens airport. The basic aim of the project was the establishment of a biometric model for the identification 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 was 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 aimed at guaranteeing that the passenger who has checked in is the same with the person who actually boards the airplane. The identity verification system is based on iris and finger biometric characteristics. The project requires a preparation or "enrolment" phase, during which volunteers prove their identity by showing an identity document and their biometric characteristics (iris and fingerprints) are collected by appropriate devices. Their biometric data are stored in smart cards along with their name, their frequent flyer number, digital signature and a unique project number. Every volunteer-passenger receives the smart card and brings it along every time s/he travels. Passengers' biometric data are stored only in smart cards, not in company's files. Each time a volunteer-passenger travels, s/he inserts the smart card in the special card reader during check-in. Then, the passenger is required to look into the special iris reading camera and/or place his/her finger on the corresponding fingerprint taking device. Thus, biometric data are each time processed and, following comparison to those stored in the passenger's smart card, his/her identity is verified. The procedure is repeated at boarding	

	card control point before boarding the airplane; inserting the smart card into the special reading device for a second time may not be required.	
Population concerned: target and age	Passengers travelling from Athens Airport	
Trends (measured / supposed)	Unknown	
Known or potentials dangers / Risks	Unnecessary processing of personal data of passengers; in case this measure adopted in the long term, unknown risks	
Others		
Generated data bases		
Associated data base/ creation (a line per database)	European-level project in which International Athens Airport, the International Air Transport Association (IATA), the International Airport at Milan and ALITALIA Airlines participate among others	
Data retention duration/ Right to be forgotten	Each passenger's biometric data are stored temporarily in a database for the time period between passenger's ticket check-in and boarding card control	
What justifies the inscription in the file /Risks?	Prior consent of the subject (pilot project on voluntary basis)	
File masters? Risks?	Private entities within the framework of an experiment[26].	
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Unknown	
Right to know or to modify data? (appeal)	Not applied	
Covert purposes/ Risks/uncontrolled future evolution	It could be argued that the method provided for by the pilot project does not mainly serve flight security requirements but organisational issues of airline companies instead.	
Others (inter-connexions, …)		
Legislation in application		
Law /rules / trends, (if implemented for this data base or this technology)	According to provisions in article 4 par. 1 of Law 2472/97, personal data, in order to be fully processed, must be collected fairly and lawfully for specific, explicit and legitimate purposes (section a) and must be adequate, relevant and not excessive in relation to the purposes for which they are processed at any given time (section b). Any personal data processing not necessary for the achievement of the purpose sought is not legitimate.	

[26] Athens International Airport S.A. was established in June 1996 in the form of a partnership involving the Greek State and a private consortium led by the German company Hochtief Aktiengesellschaft. This consortium was the winner of the tender for the airport building contractor held during 1991-1993 under a BOOT scheme (Build – Own – Operate –Transfer). The said corporate entity, entrusted with the management of "Eleftherios Venizelos" airport for 30 years, constitutes a pioneer co-operation - between the public and private sector - and the first internationally, developed with the aim to construct a major airport.

Conformity with the European right (European charter of fundamental rights - directives…)	Not in conformity with the principles of purpose and proportionality prescribed by EU legislation.	
Risks for freedoms despite the law	Unnecessary processing of biometric data	
If revision of the regulation: for which reasons? Results: improvement or aggravation (compared to the protection of the DP)	Not applied→ this project only operated for 6 months	
Others		
This tools and young public or young adults		
How far are young people concerned?	Unknown	
Awareness of issues or of risks / Indifference or reaction	Unknown	
Awareness campaigns/ results	Not applied	
Good practises	The HDPA issued decision 52/2003 according to which 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. Unnecessary personal data processing for the achievement of the purpose sought is not legitimate even when the data subject has given his/her consent according to article 5 par.1 or article 7 par. 2 section (a) of Law 2472/97 because the consent itself does not allow any act of processing contrary to the principle of purpose and necessity (decision no. 510/17/15.05.2000 of the Authority). As a result, consent does not quash the unlawful nature of the processing even when the data subject accepts exposure to biometric checks. the purpose sought with the above mentioned method is achieved in a milder way with the passenger showing the identity card along with the ticket and the boarding card.	
Campaign to be lead? On which themes		
Others		
Conclusions	Such a system is not considered necessary in order to identify passengers and the purpose exceeds the principle of proportionality	
Recommendations	To ban further attempts to use such technologies	

DNA DATABASE

Technology used/tool (For each teams, a card pro tool)	**DNA database- Genetic material and fingerprints**	
Country/ use area	Greece	
Frame of use	On July 15th 2009 an amendment in Greek legislation was discussed in the Parliament[27]. The genetic material for the DNA database will be collected obligatorily, following a court decision for everyone who brings a strong evidence of guilt, even for misdemeanor acts which result in three months prison sentence, leaving therefore outside this framework hardly any offenses mentioned in the whole the Penal Code. Until now, Article 200A of the Code of Criminal Procedure provided that genetic material could be collected under the authority of the Judicial Council and only for serious crimes. If the analysis of the DNA is negative, the genetic material and the genetic fingerprints are destroyed immediately, while in case the analysis is positive, the genetic material is destroyed immediately, but the genetic fingerprints will be retained in a special file until the death of the person concerned and will be used in investigating and solving other crimes.	
Population concerned: target and age	People prosecuted for crimes and misdemeanors	
Trends (measured / supposed)	Generated use of DNA material for crime investigation	
Known or potentials dangers / Risks	In practice, innocent people prosecuted for misdemeanors that they have not committed are treated in the same way with perpetrators of serious crimes.	
Others		
Generated data bases		
Associated data base/ creation (a line per database)	See above, recent legislative amendment	
Data retention duration/ Right to be forgotten	If the analysis of the DNA is negative, the genetic material and the genetic fingerprints are destroyed immediately, while in case the analysis is positive, the genetic material is destroyed immediately, but the genetic fingerprints will be retained in a special file until the death of the person concerned and will be	

[27] It should be noted that according to article 72§1 of the Greek constitution, bills and proposals for laws regarding individual rights should be discussed and voted in plenum and not during the summer section of the parliament.

	used in investigating and solving other crimes.	
What justifies the inscription in the file /Risks?	Fight against crime	
File masters? Risks?	The file operation is supervised by the Appeals prosecutor or deputy public prosecutor appointed by decision of the Supreme Judicial Council, for a period of two years	
Who accesses the files/ Sharing of the data base? Access limits? /Risks	The archive of genetic material will be stored in the Directorate of Criminal Investigation of the Greek Police Headquarters.	
Right to know or to modify data? (appeal)	Unknown	
Covert purposes/ Risks/uncontrolled future evolution	Unknown	
Others (inter-connexions, …)		
Legislation in application		
Law /rules / trends, (if implemented for this data base or this technology)	Law 2472/97	
Conformity with the European right (European charter of fundamental rights - directives…)	Not compliance with European law and European standards. a) Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data provides that the object of national laws on the processing of personal data is notably to protect the right to privacy as recognised both in Article 8 of the European Convention on Human Rights and in the general principles of Community law. The Directive sets out a number of principles in order to give substance to and amplify those contained in the Data Protection Convention of the Council of Europe. It allows Member States to adopt legislative measures to restrict the scope of certain obligations and rights provided for in the Directive when such a restriction constitutes notably a necessary measure for the prevention, investigation, detection and prosecution of criminal offences (Article 13). b) The Prüm Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, which was signed by several members of the European Union on 27 May 2005, sets out rules for the supply of fingerprinting and DNA data to other Contracting Parties and their automated checking against their relevant data bases. The Convention provides inter alia:	

	"Article 35 – Purpose 2. The Contracting Party administering the file may process the data supplied (...) solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording... The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned [above]." c) The Council framework decision of 24 June 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters states inter alia: "Article 5 Establishment of time-limits for erasure and review Appropriate time-limits shall be established for the erasure of personal data or for a periodic review of the need for the storage of the data. Procedural measures shall ensure that these time-limits are observed." d) article 8 of ECHR "1. Everyone has the right to respect for his private ... life ... 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society ... for the prevention of disorder or crime..." e) ECtHR jurisprudence See for example case S. AND MARPER v. THE UNITED KINGDOM according to which there has been so far no necessity for DNA records to be kept permanently by the police, maintaining DNA can not be unexceptional for all crimes and for all suspects, but there should be graduated so as not to undermine the presumption of innocence and that DNA databases are governed by the provisions for the protection of personal data.	
Risks for freedoms despite the law	According to art 3 of law 2472/97, as amended in 2007 (see card for CCTV), data protection is not implemented by courts and prosecutors in the context of detection of crimes and misdemeanors. Therefore, since the newly proposed amendment puts the operation of the DNA database under the supervision of the prosecutor, it therefore exempts the application of data protection in the processing of DNA.	
If revision of the regulation: for which		

reasons? Results: improvement or aggravation (compared to the protection of the DP)		
Others		
This tools and young public or young adults		
How far are young people concerned?	Unknown	
Awareness of issues or of risks / Indifference or reaction	Opposition by the other Greek parties did not stop the voting of this measure. The Greek DPA issued an opinion (2/2009) in July 2009 according to which the amendment contains the following positive aspects 1) the genetic material is destroyed immediately after the analysis, 2) strong evidence of guilt is required, 3) the purpose of the analysis is only the identification of the offender, 4) the analysis implies a comparison with material found in a place connected to the crime. However, the DPA also acknowledges some negative aspects and makes some recommendations in order for the amendment to fully comply with the constitution and the ECHR: 1) it should be mentioned that the analysis is not proportionate if the identification could be succeeded using other methods, 2) the Law should either mention that fingerprints only of those convicted for felony should be analysed or that only those concerning conviction for serious crimes may be retained and used in the future only for solving other crimes, 3)as far as the retention period is concerned there should be a distinction between those convicted acquitted and between minors and adults, 4) the taking and analysing of DNA should take place under the decision of the Council or at least under a special act of the Prosecutor, 5)the supervision of the procedure by the prosecutor should not exclude the control of the Authority	
Awareness campaigns/ results	Not applied	
Good practises	Not applied	
Campaign to be lead? On which themes		
Others		
Conclusions	The bill does not take any precaution, so that the taking of DNA samples respects the personality of individuals. The greatest risk, besides the creation a DNA database itself, is the generalization of receiving DNA material for any offense, even for misdemeanors of purely formal character	

Recommendations	The constitutional principle of proportionality require the legislature to restrict the taking of DNA material only to serious crimes such as homicide, organized crime, drugs, etc. and to those offenses which by their nature make necessary the taking, use and comparison of the genetic material in order to find the perpetrator that committed an act for a prosecution has already started.	

3-INTERPERSONAL COMMUNICATIONS

LAYER VOICE ANALYSIS – LIE DETECTOR

Technology used/tool (For each teams, a card pro tool)	**Layer Voice Analysis - Lie detector**	
Country/ use area	Greece	
Frame of use	A member of the dating site www.parea.gr, reported to the HDPA that on 10/6/2005 he received via e-mail a message from the administrator of the website entitled «so that no one fools you» by informing him of the existence of a new service, which is a truth detector. According to that message, someone calling from a fixed phone a 90XXXXXXX number and then the number of the person he wants to call, is given the possibility to know after the end of the conversation if the interlocutor told truth or lies. This service worked only for the period from 15/5/2005 to 4/7/2005.The used application is the Love Detector, which is based on the core application of LVA (Layer Voice Analysis) from the Nemesysco Natania Company based in Israel. The company Nemesysco develops voice analysis software for business executives, private researchers, specialists in fraud protection insurance, banking and financial institutions and the needs of people who want to see the truth in private and non-commercial affairs. The user called the number of the service in order to connect to the call center of the company Newsphone Hellas SA. Then he/she gave the number of the person who he/she wanted to communicate as well as information concerning their relationship. During the call, the conversation was recorded in a wav file and was kept in the company's system. Upon completion of the conversation, the Love Detector application processed the file by analyzing 129 vocal parameters using the method Amir	

	Liberman and announcing the result of analysis to the caller. By the end of the call the wav file that was created was deleted from the disk of the company. Information on the recording of the conversation and the subsequent treatment of his/her voice was not communicated by the service and it was up to the caller whether to inform the participant or not.	
Population concerned: target and age	Members of social site parea.gr and probably of other sites where the service was advertised. a large number of young people could be affected	
Trends (measured / supposed)	Unknown	
Known or potentials dangers / Risks	Voice is personal information when it can be associated with a specific person. According to the findings of the audit and the statements made by the managers of the company, during the recording and subsequent processing of the voice calling, the two call parties were not specific persons to the company. Additionally, since the file where the conversation was recorded, was deleted immediately after the termination of the call, it was not possible through the content of the conversation to trace the identity of the persons. The caller, however, in contrast to the company, knew whom the voice belonged to and thus automatically he/she became a controller. Furthermore, the recording and processing of the voice did not have the consent of one of the 2 participants; therefore it could be a violation of the right to privacy. Unknown how accurate and trustworthy this system is.	
Others		
Generated data bases		
Associated data base/ creation (a line per database)	Recording of a phone conversation for a short period of time	
Data retention duration/ Right to be forgotten	The file was immediately destroyed after the phone call	
What justifies the inscription in the file /Risks?	The consent of the one party involved	
File masters? Risks?	Company Newsphone Hellas S.A.	
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Unknown	
Right to know or to modify data?	Not applied	

(appeal)		
Covert purposes/ Risks/uncontrolled future evolution	Unknown	
Others (inter-connexions, …)		
Legislation in application		
Law /rules / trends, (if implemented for this data base or this technology)	Law 2472/1997, Law 3471/2006	
Conformity with the European right (European charter of fundamental rights - directives…)	Unknown, probably violating the principle of lawful processing of personal data	
Risks for freedoms despite the law	Violation of the right to privacy	
If revision of the regulation: for which reasons? Results: improvement or aggravation (compared to the protection of the DP)	Not applied	
Others		
This tools and young public or young adults		
How far are young people concerned?	See above	
Awareness of issues or of risks / Indifference or reaction	The HDPA decided to issue guidelines for the use of similar services/technologies and transferred the case to ADAE in order to decide if the privacy in telecommunications had been violated	
Awareness campaigns/ results	Not applied	
Good practises	Not applied	
Campaign to be lead? On which themes		
Others		
Conclusions	Similar services should have the consent of both parties, in compliance with law 2472/97 for the legal processing of personal information.	
Recommendations		

4-SOCIAL NETWORKS AND NEW GATE KEEPERS OF COMMUNICATIONS

ZOO.GR

Technology used/tool (For each teams, a card pro tool)	ZOO.GR	
Country/ use area	Greece	
Frame of use	Zoo.gr is a web meeting point and gaming network that became operational in 2004. Users enter this site in order to play online games, participate in tournaments and competitions playing singleplayer and multiplayer games, such as backgammon, crosswords, etc. The site also offers thematic fan clubs, i.e. on sports, music, cars etc, where users can find and upload articles, photos, videos, exchange views and chat	
Population concerned: target and age	93% of its users come from Greece, with 43% coming from the County of Attiki. 66% are men.[28] Users have to be above 18 years old.	
Trends (measured / supposed)	45% of users are between 18-24 years old and 23% between 25-29[29]In December 2008 zoo.gr had 900.000 unique visitors, which visited the website at least 7 times a month. Everyday 95.000 users enter the site in order to practice theis hobbies.[30] According to a study by Synovate on Youth Marketing and Best brands for young people in Greece (published in Adbusiness no.63), zoo.gr is the 6th most popular internet brand for young people in Greece[31]. A study on social media by the institute of communication[32] revealed that 3.5 of the persons interviewed who update their profiles at least once a month has a profile in zoo.gr	
Known or potentials dangers / Risks	Unknown	

[28] Information provided by zoo.gr
[29] Information provided by zoo.gr
[30] Information provided by zoo.gr
[31] In the same list facebook comes 2nd, youtube 5th, hi5 7th and myspace 9th. Other relevant numbers can be found in the card on hi5
[32] Study operated by the MRB Hellas SA and published on the 18th February 2009

Others	The purpose of gathering such data is to store them in a server from which they may be available to an unknown number of people through the connection of people to the website of Zoo.gr. For the purpose of storage and only the data are sent to a country outside the EU. For the registration of the user in mailing lists for the newsletters of Zoo.gr the following information is requested: Country, Postal Code, Date of Birth, Sex, E-mail. Zoo.gr may retain a record of electronic addresses of the recipients to send messages and other information beyond the Newsletters unless the recipient expressly stated that he/she does not wishes so. Zoo.gr may use cookies to identify users in some services and web pages of Zoo.gr. The user can configure the browser in such a way that it either warns him/her of the use of cookies on specific services of Zoo.gr, or prohibits the use of cookies	
Generated data bases		
Associated data base/ creation (a line per database)	Zoo.gr collects personal data of users in the following cases: A) when the user registers in the services, B) when the user creates a profile of C) when entering the promotional / advertising programs of zoo.gr and D) when using products and / or services of zoo.gr	
Data retention duration/ Right to be forgotten	Unknown	
What justifies the inscription in the file /Risks?	Zoo.gr keeps a record of the personal data of users. For this purpose zoo.gr has made a notification before the Hellenic Data Protection Authority. The user data stored in the archives of Zoo.gr are only those reported by the same subjects when registering with the Zoo.gr. The consent of the user in the terms of Zoo.gr offers the explicit consent of the subject for the processing and transmission of the subject's personal data.	
File masters? Risks?	The company ZooBytes	
Who accesses the files/ Sharing of the data base? Access limits? /Risks	ZooBytes is bound not to sell, rent or publish in any manner and / or to disclosure the data of users of Zoo.gr to any third party. The Zoo.gr cannot diffuse personal data of users to third parties unless: 1) it has the prior explicit consent of users to receive information that relates/concerns the user, 2) The legal entities and natural persons who cooperate with Zoo.gr have the right to process personal information that users submit to Zoo.gr, this only as far as it is absolutely necessary to provide technical and other support to the Zoo. gr or to serve the demands of the users and are bound by the conditions for compliance with the protection of	

	personal data,3)it is required because of compliance with the relevant provisions of law and the relevant authorities.	
Right to know or to modify data? (appeal)	Unknown	
Covert purposes/ Risks/uncontrolled future evolution	Unknown	
Others (inter-connexions, …)		
Legislation in application		
Law /rules / trends, (if implemented for this data base or this technology)	No specific legislation. Processing of data in compliance with Greek data protection legislation according to the HDPA who is informed on its operation	
Conformity with the European right (European charter of fundamental rights - directives…)	Probably in conformity with EU standards for legal processing	
Risks for freedoms despite the law	Unknown	
If revision of the regulation: for which reasons? Results: improvement or aggravation (compared to the protection of the DP)	Not applied	
Others		
This tools and young public or young adults		
How far are young people concerned?	See above targets and trends	
Awareness of issues or of risks / Indifference or reaction	Not applied	
Awareness campaigns/ results	Not applied	
Good practises		
Campaign to be lead? On which themes		
Others		
Conclusions	Data protection law is probably well applied in the case of zoo.gr, as not only the data requested for registration are the minimum but also there seems to exist no purpose of marketing through the services. So far no cases brought before the DPA concerning violation of data protection by zoo.gr	
Recommendations		

Hi5.COM

Technology used/tool (For each teams, a card pro tool)	Hi5.COM	
Country/ use area	Greece	
Frame of use	Hi5 is a social networking website founded in 2003 by Ramu Yalamanchi an Indian entrepreneur. Users create an online profile in order to show information such as interests, age and hometown and upload user pictures where users can post comments. Hi5 also allows the user to create personal photo albums and set up a music player in the profile. Members also use hi5 to send messages, and join discussion groups. Users can also send friend requests via e-mail to other users. When a person receives a friend request, he may accept or decline it, or block the user altogether. If the user accepts another user as a friend, the two will be connected directly or in the 1st degree. The user will then appear on the person's friend list and vice-versa. Some users opt to make their profiles available for everyone on Hi5 to view. Other users exercise the option to make their profile viewable only to those people who are in their network. The network of friends consists of a user's direct friends (1st degree), the friends of those direct friends (2nd degree) and the friends of the friends of direct friends (3rd degree)	
Population concerned: target and age	Hi5 is open to ages from 13 and above, target group probably between 15-30 years old. Percentage not available; numbers were asked by hi5, which did not answer to the request.	
Trends (measured / supposed)	According to Google trends[33], hi5 became popular in the end of 2005. Until the end of 2006, it ranked among the most used networks in Greece together with myspace and zoo.gr. It gained a big rise in 2007 but as from summer 2008 facebook is by far the most popular social network in Greece. Also according to Alexa.com[34], hi5 is the 23rd	

[33] Google Trends is a public web facility of Google Inc., about Google Search, that shows how often a particular search-term is entered relative to the total search-volume across various regions of the world.
[34] Alexa is a website-usage information website, belonging to Alexa Internet Inc. a subsidiary company of Amazon.com. Alexa ranks sites based on tracking information of users of its Alexa Toolbar for Internet Explorer and from integrated sidebars in Mozilla and Netscape. Once installed, the toolbar collects data on browsing behavior which is transmitted to the website where it

	most popular website in Greece. In the same list, Facebook ranks 2nd and myspace 20th. According to a study by Synovate on Youth Marketing and Best brands for young people in Greece (published in Adbusiness no.63), hi5 is the 7th most popular internet brand for young people in Greece. Another study35 reveals that 81,1% of people who use SNS and update their profiles at least once a month have a profile on facebook, 23;9% use hi5, 15;1% myspace, 9,7% youtube and 3,5% zoo.gr. Out of those having an account on facebook, 61,3% use it daily. An estimation which cannot be based on studies or statistics as such data is not available, is that hi5 users are relatively younger that facebook users.	
Known or potentials dangers / Risks	There have been phising emails posing as invitations to Hi536. Hi5 often markets the site by using unsolicited bulk mail. Often the mails will appear as user invites, but the users that have invited the spammed party are rarely known to the recipient. It is virtually impossible to get removed from these spam lists as Hi5 does not appear to respond to removal requests. Further risks include (see below): use and transfer of personal data to third parties for marketing purposes; even non-members of hi5 may view open profiles; young users are less aware of the potential dangers etc	
Others		
Generated data bases		
Associated data base/ creation (a line per database)	Data submitted by the users and collected by hi5.com.	
Data retention duration/ Right to be forgotten	Unclear	
What justifies the inscription in the file /Risks?	By submitting Personal Information through hi5 Sites, the user agrees to the terms of its Privacy Policy and expressly consents to the processing of his/her Personal Information according to this Privacy Policy. Personal Information of the user may be processed by hi5 in the country where it was collected as well as other countries (including the United States of America) where laws regarding processing	

is stored and analyzed and is the basis for the company's web traffic reporting. There is some controversy over how representative Alexa's user base is of typical Internet behavior. If Alexa's user base is a fair statistical sample of the Internet user population (*e.g.*, a random sample of sufficient size), Alexa's ranking should be quite accurate.

[35] Study on social media by the institute of communication operated by the MRB Hellas SA and published on the 18th February 2009

[36] http://securitylabs.websense.com/content/Alerts/3205.aspx

	of Personal Information may be less stringent than the laws in the country of origin of the user.	
File masters? Risks?	Data submitted by users, processor of the data is hi.com and its marketing partners under their own privacy policy (see above)	
Who accesses the files/ Sharing of the data base? Access limits? /Risks	Any visitor of the hi5 Sites, even non-members, can view the user's profile information and photos that he/she has uploaded to the hi5 community. The user can control what part of his/her profile information and photos is visible to visitors of the Sites and which network of hi5 members can see what information, but publicly posted information throughout the hi5 network can be accessed by every visitor of the Sites.	
Right to know or to modify data? (appeal)	Hi5 may remove personally identifying information from collected information to render it anonymous. hi5 may use Anonymous Information for any purpose and disclose Anonymous Information in its discretion. hi5 may (but is not obligated to) review any Content, that is uploaded, published or displayed on its Services and delete or refuse to take online any such Content, including, without limitation, any Content that in the sole judgment of hi5 violates its Agreement with the user or which might be offensive, inappropriate, illegal, or that might violate the rights, harm, or threaten the safety of other Members or third parties	
Covert purposes/ Risks/uncontrolled future evolution	Purpose of the service is to offer a platform for electronic sharing of personal data and social contacts. It is also used for advertising and marketing purposes. By posting any content communication, information, Intellectual Property, material, messages, photos, videos, URLs, profiles and the like (collectively, "Content") any area of the Services of hi5, the user automatically grants, and represents and warrants that he/she has the right to grant, to hi5 an irrevocable, perpetual, non-exclusive, royalty-free and fully paid, worldwide license to reproduce, distribute, publicly display and perform (including by means of a digital audio transmission), and otherwise use Content and to prepare derivative works of, or incorporate into other works, such Content, and to grant and authorize sublicenses of the foregoing.	

	Content from other Members, advertisers, and other third parties may be made available to the user through the Services of hi5. However hi 5 states that it does not control such Content and that , (a) the user agrees that hi5 is not responsible for any such Content and (b) hi5 makes no guarantees about the accuracy, currency, suitability, or quality of the information in such Content, and it assumes no responsibility for unintended, objectionable, inaccurate, misleading, or unlawful Content made available by other Members, advertisers, and other third parties. Hi5 provides Personal Information to third party service providers who work on behalf of or with hi5 under confidentiality agreements. These service providers may use personal information to communicate with users about offers and services from hi5 and its marketing partners. However, these service providers do not have any independent right to share this information. The handling of Personal Information by partners or the third-party advertising companies is governed by their privacy policy, not the one of hi5 Hi5 also uses third-party advertising companies to serve advertisements when users visit its Sites. These companies may use Personal Information, such as gender or age, and other information (not including name, address, email address or telephone number) about user's visits to the Sites and other websites, such as time of day of the login, IP address or information about the internet service provider (ISP) or mobile device Carrier, in order to provide advertisements on the Sites As the user navigates the Sites, certain information may also be passively collected and stored on its server logs, including Internet protocol address, browser type, and operating system. If the user sends SMS, MMS, or text messages to the Services, hi5 will collect the telephone number (if any) from which such communication was sent. It also uses Cookies and navigational data like Uniform Resource Locators (URL) to gather information regarding the date and time of the user's visit and the solutions and information for which he/she searched and viewed, or on which of the advertisements displayed on the Sites he/she clicked. Hi5 reserves the rights to use the user's profile	

	information and photos on its Sites and when it sends emails, for example when for birthday reminders to hi5 members or when it sends general newsletters to members of the hi5 community Hi5 states that it does not intentionally gather Personal Information about visitors who are under the age of 13 and according to its terms of services, a person accessing and using its services, is certifying that it is at least 13 years old.	
Others (inter-connexions, …)		
Legislation in application		
Law /rules / trends, (if implemented for this data base or this technology)	No specific legislation adopted	
Conformity with the European right (European charter of fundamental rights - directives…)	Processing of the data probably not meeting European standards	
Risks for freedoms despite the law	Data included in social network database can be misused for profiling, collecting of personal information by third parties, minors who use hi5 are not fully aware if the risks.	
If revision of the regulation: for which reasons? Results: improvement or aggravation (compared to the protection of the DP)		
Others	Recently 2 cases regarding the use of social networks (in particular facebook) for illegitimate reasons, have been brought before the Greek courts. The first one is a case of a fake profile created for the defamation of a member of the academic staff of the University. The second is also a case of defamation involving the unauthorised use of photos of a person in an open profile in facebook.	
This tools and young public or young adults		
How far are young people concerned?	According to a study realised by the Greek Information Society Observatory in May 2008[37] 93% of children between 10-15 use the internet, 27% of which use hi5.	
Awareness of issues or of risks / Indifference or reaction	Unknown	
Awareness campaigns/ results	No awareness campaign on the risks of using social networks.	
Good practises	hi5.com created a document addressed to	

[37] This study was a pilot project, which means that the sample used was quite limited (about 300 children)

	teens regarding online safety for teens. This document however does not specifically refer to the risk for use of theirs personal data by third parties. The study on Social media by the Institute of Communication, is a first necessary step to gather information and analyse the current situation about the use of social networks and other social media in Greece	
Campaign to be lead? On which themes	A comprehensive campaign on social networks and ways to protect personal data on the internet should be envisaged	
Others	The Greek DPA also offers information on social networking in its website. This column consists in a kind of warning for social network users, with links to important documents. The part of the website addressed to children is more general and talks about general dangers for privacy resulting from the Internet.	
Conclusions	Hi5 has an obvious marketing purpose; it is however uncertain whether its users and especially minors are aware of it.	
Recommendations	The Greek DPA or the civil society should lead a campaign in order to inform youngsters on the use of social media and the relevant risks	