GOVERNMENT GAZETTE
OF THE HELLENIC REPUBLIC
FIRST VOLUME

Issue no. 113
June 28, 2006

LAW 3471

Protection of personal data and privacy in the electronic telecommunications sector and amendment of law 2472/1997.

**THE PRESIDENT
OF THE HELLENIC REPUBLIC**

Issues the following law, as voted by the Parliament:

CHAPTER A

Protection of personal data and privacy in the electronic telecommunications sector (Incorporation of Directive 2002/58/EC by the European Parliament and Council of the 12th July 2002 on the processing of personal data and the protection of privacy in the electronic telecommunications sector, EE L 201/37, of the 31st July 2002).

Article 1

Object

The object of articles 1 to 17 of the present law is the protection of fundamental human rights and privacy in particular, and the institution of the conditions for the processing of personal data and the reservation of communication confidentiality in the field of electronic telecommunications.

Article 2

Definitions

Apart from the definitions included in article 2 of law 2472/1997 (Government Gazette 50A), as effective, and taking into consideration the definitions of law 3431/2006 (Government Gazette 13A), for the purposes of this law the following are understood as:

1. "Subscriber": Natural or legal persons who have signed an agreement with a public telecommunication services provider, for the provision of these services.
2. "User": Any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service.
3. "Traffic data": Any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Traffic data may, *inter alia*, consist of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network.
4. "Location data": Any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.
5. "Communication": Any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information.
6. "Call": A connection established by means of a publicly available telephone service allowing two-way communication in real time.
7. "Value added service": any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.
8. "Electronic mail": Any text, voice, sound or image message sent over a public communications network which

can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

9. "Electronic communications services": Any services offered, usually upon remuneration, whose provision consists, fully or partially, of the transmission of signals to electronic communications networks, including telecommunications services and transmission services to networks used for radio transmissions. Electronic communications do not include services for the provision or control of context transmitted through electronic communications networks and services, as well as Information Society services, as these are described in par. 2, art. 2 of D 39/2001 (Government Gazette 28A) and that do not concern, fully or partially, the transmission of signals to electronic communications networks.
10. "Public communications network": Any communications network used, fully or mainly, for the provision of publicly available electronic communications services.
11. "Publicly available electronic communications services": Any publicly available electronic communications services.

Article 3
Scope

1. Articles 1 to 17 of the present law shall apply to the processing of personal data and the reservation of privacy in communications, in connection with the provision of publicly available electronic communications services in public communications networks. The processing of personal data in connection with the provision of not publicly available electronic communications services shall be governed by law 2472/1997 (Government Gazette 50A), as effective.
2. Law 2472/1997 (Government Gazette 50A), as effective and the laws in execution of Art. 19 of the Constitution, as effective, shall apply to all matters in connection with the provision of electronic communications services that are not regulated explicitly by the present law.

Articles 8, 10 and 11 shall apply to subscriber lines connected to digital exchanges and, where technically possible and if it does not require a disproportionate economic effort, to subscriber lines connected to analogue exchanges. The National Telecommunications and Postal Services Committee (EETT) shall identify cases where connection to digital exchanges would be technically impossible or require a disproportionate economic effort and notify the Commission thereof.

Article 4
Confidentiality

1. Any use of electronic communications services offered through a publicly available electronic communications network, as well as the pertinent traffic and location data, as described in art. 2 of the present law, shall be protected by the principle of confidentiality of telecommunications.
   The withdrawal of confidentiality shall be allowed only under the procedures and conditions provided for in Art. 19 of the Constitution.
2. Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic and location data is prohibited, except when legally authorised.
3. The legally authorised recording of communications and the related traffic data is allowed when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication, under the condition that both parties have provided their consent in writing, upon previous notification as to the aim of the recording. An act by the Data Protection Authority defines the manner in which parties are notified and provide consent, as well as the manner and duration of storage for the recorded conversations and relevant traffic data.
4. With the reservation of complying with the obligations arising from the protection of confidentiality, according to the present law, technical storage is allowed, where necessary for the conveyance of the transmission.
5. Electronic communications networks may not be used to store information

or to gain access to information stored in the terminal equipment of a subscriber or user, particularly with the use of spyware, hidden identifiers or other similar devices. Exceptionally, any technical storage or access is permitted, when its sole purpose is to carry out or facilitate the conveyance of information through an electronic communications network, or when strictly necessary for the provision of information society services explicitly requested by the user or subscriber. In this last case, the use of such devices is only allowed if the user or subscriber is offered clear and comprehensive information, according to art. 11, law 2472/1997, as effective, and the data controller has offered the user or subscriber the right to refuse this processing. An act by the Data Protection Authority analytically defines the manner in which information, refusal rights and consent applications are provided.

Article 5
Processing regulations

1. The processing of personal data, including traffic and location data, must be limited to those absolutely necessary to serve the aims thereof.
2. The processing of personal data is only allowed if:

a. The user or subscriber has provided consent upon notification as to the type of data, the aim and extent of their processing and the recipient or categories of recipients, or

b. This processing is necessary for the implementation of the agreement to which the user or subscriber is party, or to take measures, during the pre-agreement stage, upon application by the subscriber.

3. In cases where the present law requires the user or subscriber's consent, the pertinent statement is provided in writing or electronically. In the latter case, the processing controller assures that the user or subscriber acts in full awareness of the consequences of their statement, which is recorded in a secure manner, can be accessed by the user or subscriber at any time and may be revoked.
4. The provider of the public network or the publicly available electronic communication service may not use personal data or traffic and location data or transmit these to third parties for other purposes, unless the user or subscriber has provided explicit and specific consent. This excludes purposes relating to the provision of electronic communication services or the provision of added value services requested by the user or subscriber, such as advertisement or market research for goods or services.
5. As regards traffic data, the service provider must inform the users or subscribers, prior to obtaining their consent, of the type of traffic data which will be processed and the duration of the processing.
   When data are transmitted to third parties, consent must be provided in writing. Providers of public network or publicly available electronic communication service shall not be regarded as third parties, as regards their reception of traffic data from a corresponding provider, with the sole purpose of billing for the provided services, under the condition that the user or subscriber will have been informed in writing during the signature of the agreement. Consent may be revoked at any time. If revoked, and provided that the data have been disclosed to third parties in the meantime, this revocation is announced to them by the data controller. The provider of the public network or the publicly available electronic communication service may not depend the provision of these services to the user or subscriber on their consent to the processing of this data for purposes other than those that directly serve the provision of services regulated by articles 1 to 17.
6. The main criterion in the design and selection of the technical means and IT systems, as well as the equipment for the provision of publicly available electronic communication services, must be the minimum required personal data.
7. The publicly available electronic communication service provider must, to the extent that this is technically possible, enable the use and payment of services anonymously or by user name. The National Telecommunications and Postal Services Committee (EETT) shall

judge in case of disputes on the technical competence of using these services anonymously or by user name and the payment thereof.

Article 6
Traffic and location data

1. Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous, using the appropriate encoding, when no longer needed for the purpose of the transmission of a communication without prejudice to paragraph 2 of this Article and paragraph 5 of Article 5.
2. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. The electronic communication service provider shall inform the subscriber as to the type of data to be processed and the duration of processing. Such processing is permissible only up to the end of the period during which the bill may be lawfully challenged or payment pursued.
3. The processing of location data relating to users or subscribers to networks or publicly available electronic communication services for the provision of added value services is only permitted if these are rendered anonymous, using the appropriate encoding, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of an added value service. The service provider must inform the users or subscribers, prior to obtaining their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the possibility, during each network or connection or communication transmission, to withdraw their consent for the processing of traffic data at any time, using a simple means and free of charge.
4. Exceptionally, location data processing is permitted, without the user's or subscriber's prior consent, by the providers of a public communications network or publicly available electronic communications service, in order to assist organisations dealing with emergency calls, including law enforcement agencies, ambulance services and fire brigades, for the sole purpose of locating the caller and responding to such calls. The procedures, manner and all other technical details pertaining to the implementation of the present provision shall be described in an act by the Hellenic Authority for the Information and Communication Security and Privacy (ADAE).
5. Paragraphs 1 and 2 do not apply when the National Telecommunications and Postal Services Committee (EETT) is informed by the interested parties on traffic data, with the aim of resolving disputes relating mainly to interconnection or payments, according to effective legislation.

Article 7
Itemised billing

1. Subscribers shall have the right to receive non-itemised bills. When a connection is used by numerous users, or when the subscriber is liable for the payment of a connection used by multiple users, the subscriber must provide a statement that the users have been informed or shall be informed, in the most appropriate manner in each case, as to the itemised billing of the subscriber. In the case of toll-free communication, the connection called shall not be included in the itemised billing.
2. If so requested by the subscriber, the provider of a public communications network or publicly available electronic communications service must erase the three last digits of the called connections-numbers from the itemised bill.

Article 8
Presentation and restriction of calling and connected line identification

1. Where presentation of calling line identification is offered, the service

provider must offer the calling user the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification on a per-call basis. The calling subscriber must have this possibility on a per-line basis.

2. Where presentation of calling line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification of incoming calls.
3. Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the service provider must offer the called subscriber the possibility, using a simple means, of rejecting incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.
4. Where presentation of connected line identification is offered, the service provider must offer the called subscriber the possibility, using a simple means and free of charge, of preventing the presentation of the connected line identification to the calling user.
5. Paragraph 1 shall also apply with regard to calls to third countries outside the European Community. Paragraphs 2, 3 and 4 shall also apply to incoming calls originating in third countries.
6. The opportunities provided by paragraphs 1 to 4 are offered to the electronic communications service provider. Where presentation of the calling or connected line identification is offered, publicly available electronic communications service providers must inform the public and their subscribers, using all appropriate means and methods, regarding the existence of calling or connected line identification services, based on the identification of the calling or connected line and the possibilities described in paragraphs 1 to 4.
7. The provider of a public communications network or publicly available electronic communications service must have means to cancel the calling line non-identification option:

a. On a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls. In this case, the data containing the identification of the calling subscriber or user will be stored and be made available by the provider of a public communications network and/or publicly available electronic communications service only to the subscriber or user who has requested the identification and are subsequently erased, unless otherwise determined by the present law.

   The specific procedures, manner, duration of the option's cancellation and all other necessary details to secure the procedure's transparency shall be described in an act by the Hellenic Authority for the Information and Communication Security and Privacy (ADAE).
b. For emergency calls to the competent public organisations dealing with such calls or to private emergency assistance organisations, recognised by the State, for the purpose of responding to such calls, irrespectively of the existence of the subscriber or user's temporary consent. In this case, the data containing the identification of the calling subscriber will be stored and be made available by the public organisation or private emergency assistance organisation for the sole purpose of immediately replying and dealing with the emergency and only for the period required to complete this purpose, and are subsequently erased.

   The procedures, manner and all other technical details pertaining to the implementation of the present provision shall be described in an act by the Hellenic Authority for the Information and Communication Security and Privacy (ADAE).
c. For calls subject to withdrawal of caller identification restriction, according to the effective legislation.

Article 9
Automatic call forwarding

Subscribers have the right to stop call forwarding by third parties to their terminal. The provider of a public communications network or publicly available electronic

communications service must offer this technical option free of charge.

Article 10
Directories of subscribers

1. Subscribers shall be informed, free of charge, in an appropriate and comprehensive manner, about the purposes of a printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services, in which their personal data can be included. Subscribers shall also be informed of any further usage possibilities based on search functions embedded in electronic versions of the directory. Subscribers are notified before they are included in the directory.
2. The personal data contained in the printed or electronic directory of subscribers available to the public or obtainable through directory enquiry services must be limited to those that are necessary for the identification of a specific subscriber (name, surname, father's name, address), unless the subscriber has provided written consent for the publication of complemental personal data.
3. Subscribers shall be given the option not be included in a printed or electronic directory. Subscribers are included in the directory, if they have not expressed their refusal, upon notification of paragraph 1 of the present article. Subscribers may also request that their address is only partially displayed and that their sex is not revealed, if linguistically possible. The non-registration, verification, correction or withdrawal of personal data from the public subscribers directory is free of charge.
4. The personal data include in the public directory may only be processed for the purposes for which they have been collected. Where these data are transmitted to one or more third parties, the subscriber should be informed, before the transfer, as to this possibility and as to the recipient or categories of possible recipients and must have the opportunity to oppose the transfer. If the party collecting the data from the subscriber or any third party to whom the data have been transmitted wishes to use the data for an additional purpose, the renewed consent of the subscriber is to be obtained. The provider of the public subscriber directory may not depend on the provision of the public subscriber directory services to the subscriber on their consent to the processing of this data for purposes other than those for which they have been collected.
5. The rights provided by paragraphs 1 , 2 and 3 apply to natural subscribers. Where the subscriber is a legal entity, the data published in the public subscriber directory are limited to those necessary to ascertain the identity of the legal entity (title or trading name, seat, legal form, address), unless the legal representative of the legal entity has provided written consent on the publication of complemental data.

Article 11
Unsolicited communications

1. The use of automated calling systems with or without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail, for the purposes of direct marketing of goods or services, or any advertising purposes, may only be allowed in respect of subscribers who have given their prior consent.
2. Unsolicited communications may not be established for the above purposes, if the subscriber has stated to the provider of a publicly available electronic communications service that they do not wish to accept such communications in general. The provider must enter these statements in a special subscriber directory, which shall be at the subscriber's disposal, free of charge.
3. Where a natural or legal person obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, the same natural or legal person may use these electronic contact details for direct marketing of its own similar products or services provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such collection and use of electronic contact details when they are collected and on the occasion of each message in case

the customer has not initially refused such use.

4. The practice of sending electronic mail for purposes of direct marketing of goods and services, disguising or concealing the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, shall be prohibited.
5. The above regulations also apply to subscribers who are legal entities.

Article 12
Security

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures, if necessary, shall be taken jointly with the provider of public electronic communications services and shall ensure a level of security appropriate to the risk presented.
2. In case of a particular risk of a breach of the network's security, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk. Where the risk lies outside the scope of the measures to be taken by the service provider, they must also inform the subscribers of any possible remedies, including an indication of the likely costs involved.
3. The processing of the users' and subscribers' personal data, as well as the relevant traffic, location and billing data, must be assigned to persons acting under the authority of providers of the public communications networks and publicly available electronic communications services, handling billing or traffic management, customer enquiries, fraud detection, marketing the provider's electronic communications services or providing a value added service, and must be restricted to what is necessary for the purposes of such activities.

Article 13

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

1. By virtue of the powers vested in it by law 2472/1997, the Data Protection Authority is also competent for the application of the present law, as effective.
2. By virtue of the powers vested in it by law 2472/1997, the Hellenic Authority for the Information and Communication Security and Privacy is also competent for the application of the present law, as effective.
3. In cases where the opinion of the National Telecommunications and Postal Services Committee (EETT) is required, this is issued upon request by the subscriber or the Data Protection Authority or ex officio.
4. In cases of breach of articles 1 to 17 of the present law, whose application falls within the jurisdiction of the Data Protection Authority, this imposes the administrative penalties provided by art. 21 of law 2472/1997. In cases of breach of the present law, whose application falls within the jurisdiction of the Hellenic Authority for the Information and Communication Security and Privacy, this imposes the administrative penalties provided by art. 11 of law 3115/2003. The acts of the Data Protection Authority and the Hellenic Authority for the Information and Communication Security and Privacy that apply these administrative penalties to the providers of a public communications network or publicly available electronic communications services must be forwarded to the National Telecommunications and Postal Services Committee (EETT).
5. A joint act by the Data Protection Authority and the Hellenic Authority for the Information and Communication Security and Privacy shall regulate issues relating to the operations executed in the systems of electronic communications service providers for the correlation of their subscribers' ID with the relevant communication data.

Article 14
Civil Liability

1. Any natural person or legal entity of private law, who in breach of this law,

causes material damage shall be liable for damages in full. If the same causes non pecuniary damage, s/he shall be liable for compensation.

2. The compensation payable according to article 932 of the Civil Code for non pecuniary damage caused in breach of this law is hereby set at the amount of at least ten thousand euro (10,000 €), unless the plaintiff claims a lesser amount. Such compensation shall be awarded irrespective of the claim for damages.

3. The claims referred to in the present Article shall be litigated according to articles 664-676 of the Code of Civil Procedure, notwithstanding whether the Data Protection Authority has issued a relevant decision on the ascertainment of criminal activities or criminal charges.

Article 15
Penal Sanctions

1. Anyone who unlawfully interferes in any way whatsoever with a personal data file of a subscriber or user, or takes notice of such data or extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorised persons or permits such persons to take notice of such data or anyone who exploits such data in any way whatsoever, will be punished by imprisonment for a period of at least one (1) year and a fine amounting between ten thousand euro (10,000€) and one hundred thousand euro (100,000€), unless otherwise subject to more serious sanctions.

2. Any Controller or representative thereof who does not comply with the acts of the Data Protection Authority imposing the administrative penalties of provisional licence revocation, file destruction or interruption of processing of the pertinent data, will be punished by imprisonment for a period of at least two (2) years and a fine amounting between twelve thousand euro (12,000€) and one hundred twenty thousand euro (120,000€).

3. If the perpetrator of the acts referred to in the previous paragraphs of this article purported to gain unlawful benefit on his/her behalf or on behalf of another person or to cause harm to a third party, then s/he shall be punished with confinement in a penitentiary for a period of up to ten (10) years and a fine amounting between fifteen thousand euro (12,000€) and one hundred fifty thousand euro (150,000€). If this endangers the free operation of the democratic constitution or national security, the perpetrator shall be punished with confinement in a penitentiary and a fine amounting between fifty thousand euro (50,000€) and three hundred fifty thousand euro (350,000€).

4. If the perpetrator of the acts committed these by negligence, then s/he shall be punished with confinement in a penitentiary for a period of up to eighteen (18) months and a maximum fine of ten thousand euro (10,000€).

Article 16
Transitional agreements

Article 10 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the national provisions adopted pursuant to this law enter into force.

Where the personal data of subscribers to fixed or mobile public voice telephony services have been included in a public subscriber directory in conformity with provisions in pursuance of this law enter into force, the personal data of such subscribers may remain included in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information about purposes and options in accordance with Article 10 of this law.

Article 17
Annulled provisions

Law 2774/1999 (Government Gazette 287 A) is annulled when the present comes into force.

CHAPTER TWO

Modification of law 2472/1997
(Government Gazette 50 A)

Article 18

1. The second paragraph of art. 2 of law 2472/1997 is replaced as follows:

b. "Sensitive data" shall mean the data referring to racial or ethnic origin, political

opinions, religious or philosophical beliefs, membership to a trade-union, health, social welfare and sexual life, criminal charges or convictions as well as membership to societies dealing with the aforementioned areas.

2. The fifth paragraph of art. 2 of law 2472/1997 is replaced as follows:

e) "Personal Data File" ("File") shall mean any structured set of personal data which are accessible on the basis of specific criteria.

Article 19

1. The second point of paragraph 3 of art. 3 of law 2472/1997 is annulled. The third point of paragraph 3 of art. 3 of law 2472/1997 is presented as second.

2. The first point in the new second point (former third pint) of paragraph 3 of art. 3 of law 2472/1997 is modified as follows:
"By a Controller who is not established in the territory of a member-state of the European Union or of a member of the European Economic Area (EEA) but in a third country and who, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the Greek territory, unless such equipment is used only for purposes of transit through such territory".

Article 20

1. The last point of section 4 paragraph 1 of art. 4 of law 2472/1997 is annulled.
2. The first point of paragraph 2 of art. 4 of law 2472/1997 is modified as follows:
"It shall be for the Controller to ensure compliance with the provisions of the previous paragraph. Personal data, which have been collected or are being processed in breach of the previous paragraph, shall be destroyed, such destruction being the Controller's responsibility".

Article 21

1. The second point of section 1 of paragraph 2 of art. 6 of law 2472/1997 is annulled.

Article 22

1. The second point of paragraph 2 of art. 7 of law 2472/1997 is modified as follows:
"Processing is necessary to protect the vital interests of the data subject or the interests provided for by the law of a third party, if s/he is physically or legally incapable of giving his/her consent".

2. The last point of paragraph 3 of art. 7 of law 2472/1997 is annulled.

Article 23

1. The first point of section 4 of paragraph 1 of art. 7A of law 2472/1997 is modified as follows:
"When the processing involves medical data and is carried out by doctors or other persons rendering medical services a, provided that the Controller is bound by medical confidentiality or other obligation of professional secrecy, provided for in Law or code of practice, and data are neither transferred nor disclosed to third parties".

2. The fifth point of paragraph 1 of art. 7A of law 2472/1997 is modified as follows:
"When the processing is carried out by lawyers, notaries, unpaid land registrars and court officers or companies formed by the aforementioned and involves the provision of legal services to their clients, provided that the Controller and the members of the companies are bound by an obligation of confidentiality imposed by Law and that data are neither transferred nor disclosed to third parties, except for those cases where this is necessary and is directly related to the fulfilment of a client's mandate".

Article 24

1. The first paragraph of art. 9 of law 2472/1997 is replaced as follows:
"1. The transfer of personal data is permitted:
The transfer of personal data is permitted:

a) for member-states of the European Union,

b) for a non-member of the European Union following a permit granted by the Authority if it deems that the country in question guarantees an adequate level of protection. For this purpose it shall particularly take into account the nature of the data, the purpose and the duration of the processing, the relevant general and particular rules of law, the codes of conduct, the security measures for the

protection of personal data, as well as the protection level in the countries of origin, transit and final destination of the data. A permit by the Authority is not required if the European Commission has decided, on the basis of the process of article 31, paragraph 2 of Directive 95/46/EC of the Parliament and the Council of 24 October 1995, that the country in question guarantees an adequate level of protection, in the sense of article 25 of the aforementioned Directive".

2. Case ii of point b of paragraph 2 art. 9 of law 2472/1997 is replaced as follows:
"ii. for the conclusion and performance of a contract between the data subject and the Controller or between the Controller and a third party in the interest of the data subject".

3. A further point 6 is added after point 5 of paragraph 2 art. 9 of law 2472/1997:
"The Controller shall provide adequate safeguards with respect to the protection of the data subjects' personal data and the exercise of their rights, when the safeguards arise from conventional clauses which are in accordance with the regulations of the present law. A permit is not required if the European Commission has decided, on the basis of article 26, paragraph 4 of Directive 95/46/EC, that certain conventional clauses offer adequate safeguards for the protection of personal data".

4. Paragraph 3 of art. 9 of law 2472/1997 is replaced as follows:
"3. In the cases referred to in the preceding paragraphs, the Authority shall inform the European Commission and the respective Authorities of the other member-states a) when it considers that a specific state does not ensure an adequate protection level and b) for the permits granted pursuant to paragraph 2, point f."

Article 25

1. Point 3 of paragraph 3 of art. 10 of law 2472/1997 is replaced as follows:
"Without prejudice to other provisions, the Authority shall offer instructions and issue regulations in accordance with article 19 paragraph 1 k involving the level of security of data and of the computer and information infrastructure, the security measures that are required for each category and processing of data as well as the use of technology for the strengthening of privacy".

Article 26

The following cases are added to par. 2, art. 12 of law 2472/1997. These are numbered as follows:
"e) The correction, deletion or locking of data, the processing of which is not in accordance with the provisions of the present law, especially due to the incomplete or inaccurate nature of data and
f) The notification to third parties, to whom the data have been announced, of any correction, deletion or locking which is carried out in accordance with case (e), taken that the notification is not impossible or does not demand disproportionate efforts".

Article 27

2. Case h of paragraph 1 art. 19 of law 2472/1997 is replaced as follows:
"h. It shall proceed *ex officio* or following a complaint to administrative reviews, in the framework of which the technological infrastructure and other means, automated or not, supporting the processing of data are reviewed. It shall have, to that effect, the right of access to personal data and the right to collect any kind of information for the purposes of such review, notwithstanding any kind of confidentiality. Exceptionally, the Authority shall not have access to identity data relating to associates and contained in files kept for reasons of national security or for the detection of particularly serious crimes. Such review is carried out by one or more members of the Authority or an employee of the Secretariat, duly authorised to that effect by the President of the Authority. In the course of reviewing files kept for reasons of national security the President of the Authority shall be present in person."

Article 28

2. Case m of paragraph 1 art. 19 of law 2472/1997 is replaced as follows:
"m. It shall examine the complaints of data subjects relating to the implementation of the law and the protection of the applicants' rights when such rights are affected by the processing of data relating

to them. It shall also examine applications by the Controller requesting checks on the lawfulness of such processing. The Authority can file applications or complaints which are deemed broadly vague, unfounded or are submitted misappropriately or anonymously. The Authority shall notify the data subjects and the applicants of its actions."

Article 29

Case o is added after case n in paragraph 1 of art. 19 of law 2472/1997:
"o. It carries out an independent review of the national section of the Schengen Information System, pursuant to article 114, paragraph 1 of the Convention Implementing the Schengen Agreement(Law 2514/1997, Official Gazette 140 A), it exercises the duties of the national supervisory authority as laid down in article 23 of the EUROPOL Convention (Law 2605/1998, Official Gazette 88 A) and the duties of the national supervisory authority as laid down in article 17 of the Convention for the use of Information Technology for customs purposes (Law 2706/1999, Official Gazette 77 A), as well as the duties that arise from any international agreement".

Article 30

Case e of paragraph 1 of art. 21 of law 2472/1997 is replaced as follows:
"e. the destruction of the file or a ban of the processing and the destruction, return or locking of the relevant data".

Article 31
Entry into force

1. The provisions of this law shall enter into force on the date the present law is published in the Official Gazette, with the exception of the provisions of the First Chapter, which shall enter into force a month after its publication in the Official Gazette.

We ordered the publication of the present in the Official Gazette and its execution as a law of the State.

Athens, June 27, 2006

The president of the Hellenic Republic
KAROLOS GR. PAPOULIAS

THE MINISTERS

INTERIOR, PUBLIC ADMINISTRATION AND DECENTRALISATION
P. PAVLOPOULOS

ECONOMY AND FINANCIAL AFFAIRS
G. ALOGOSCOUFIS

JUSTICE
A. PAPALIGOURAS

TRANSPORT AND COMMUNICATION
MG LIAPIS

PUBLIC ORDER
V. POLYDORAS

Certified and stamped with the Official Stamp of the State

Athens, June 28, 2006

THE MINISTER OF JUSTICE
A. PAPALIGOURAS