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 communications 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 communications 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 communications 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 establishment of the conditions for the processing of personal data and the reservation of communication confidentiality in the electronic communications sector.

Article 2
Definitions

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

1. "subscriber": Natural or legal persons who have signed a contract with a provider of publicly available electronic communications services, 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 or by an electronic communications service that indicate the geographic location of the terminal equipment of a user of a publicly available electronic communications service.[1]
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 those cases in which the information can be related to the identifiable subscriber or user receiving the information.
6. "value added service": any service which requires the processing of traffic or location data apart from those that are required for the communications transmission or the billing thereof.[2]

[1] Point 4 was replaced as above by art. 168, par. 1 point a of law 4070/2012 (Official Gazette A' 82/10.4.2012).
[2] Point 6 was deleted and points 7-11 were renumbered to points 6-10 as above, pursuant to art. 168, par. 1 point b of law 4070/2012 (Official Gazette A' 82/10.4.2012).

7. “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.
8. “electronic communications services”: Any services offered, usually upon remuneration, the provision of which 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 (GGB 28A) and that do not concern, fully or partially, the transmission of signals to electronic communications networks. “Short messages (SMS), multimedia messages (MMS) and other similar applications are included n this definition.”[3]
9. “Public communications network”: Any communications network used, fully or mainly, for the provision of publicly available electronic communications services.
10. “Publicly available electronic communications services”: Any publicly available electronic communications services.
11. “‘personal data breach”: The security breach that leads to accidental or unlawful destruction, loss, distortion, unauthorized dissemination or unauthorized access of personal data that were transferred, stored or were subject to processing in any other manner in connection with the provision of a publicly available electronic communications service.”[4]

Article 3
Scope

“1. Provisions of articles 1 to 17 of the present law shall apply to the processing of personal data and the ensuring of secrecy in communications, within the framework of the provision of publicly available electronic communications services in public communications networks including those that support devices for data collection and identification. Law 2472/1997 (GGB 50A) shall apply, as effective, to the processing of personal data within the framework of not publicly available networks and electronic communications services.”[5]
2. Law 2472/1997 (GGB 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.
3. Articles 8 and 9 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 analogue 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 Personal 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.

---

[3] Section within inverted commas “” was added to point 8 pursuant to art. 168, par. 1 point c of law 4070/2012 (Official Gazette A’ 82/10.4.2012).
[4] Point nr 11 was added as above, pursuant to art. 168, par. 1 point d of law 4070/2012 (Official Gazette A’ 82/10.4.2012).
[5] Par. 1 was replaced as above by art. 169 of law 4070/2012 (Official Gazette A’ 82/10.4.2012).

"5. The storage of data or gaining access to information already stored in the terminal equipment of a subscriber or user is only allowed if the specific subscriber or user has given his/her consent following clear and detailed information, according to art. 11, par. 1 of law 2472/1997, as effective. The consent of the subscriber or user can be given by means of appropriate settings in the web browser or by means of another application. The aforementioned shall not impede any technical storage or access, the sole purpose of which is the conveyance of information through an electronic communications network, or which is necessary for the provision of information society services explicitly requested by the user or subscriber. An act by the Personal Data Protection Authority analytically defines the manner in which information is provided and consent is declared."[6]

Article 5
Processing rules

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

a. The subscriber or user has given consent upon notification as to the type of data, the purpose and extent of the processing, the recipients or categories of recipients, or
b. The processing is necessary for the implementation of the agreement to which the user or subscriber is a party, or the measure-taking, during the pre-agreement stage, following an application by the subscriber.

3. In cases where the present law requires the subscriber's or user's consent, the relevant statement is given in writing or by electronic means. In the latter case, the controller ensures that the subscriber or user acts in full awareness of the consequences of his/her statement, which is recorded in a secure manner, can be accessed by the user or subscriber at any time and can be withdrawn at any time.
4. The design and selection of technical means and information systems as well as the equipment for the provision of publicly available electronic communications services must be performed with the processing of the minimum personal data as the main criterion.
5. The provider of publicly available electronic communications services must enable the use and the payment of services anonymously or by pseudonym, to the extent that this is technically feasible and subject to law 3783/2009 (Official Gazette A' 136/7.8.2009), as effective. In case of a dispute, the National Telecommunications and Postal Services Committee (EETT) shall deliver an opinion on the technical feasibility of paying these services anonymously or by pseudonym".[7]

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 at the end of the transmission of a communication, subject to law 3917/2011 (A' 22) and paragraphs 2-6 of the present article.
2. For the subscriber's billing and interconnection payment, if it is necessary, the provider of a public network or publicly available electronic communications services is allowed to process traffic data. The electronic communications service provider shall inform the subscriber as to the type of the traffic data to be processed and the duration of processing. This processing for the purposes of billing and payment is permitted only up to 12 months from the day of transmission of communication, unless the bill has lawfully been challenged or the payment has not been settled. In that case processing is permitted until the irrevocable resolution of the dispute. The transfer of traffic data to another provider of a public network or publicly available electronic communications service is permitted for the purpose of billing the services provided, under the condition that the subscriber or user is informed in an appropriate and express manner in writing or by electronic means in the agreement stage or before the transfer. Similarly, the transfer of the necessary traffic data and the personal data that are related to the agreement is permitted for the only purpose of the collection of the bill payment under the condition that the subscriber or user is informed in an appropriate and express manner in writing or by electronic means in the agreement stage or before the transfer.
3. For the commercial promotion of the electronic communications services or for the provision of value added services the provider of a publicly available electronic communications service can process the traffic data to the extent and the duration needed, correspondingly, only if the subscriber or user has previously given his/her consent after he/she had been informed about the type of traffic data that are subject to processing as well as the duration of processing. The consent can be withdrawn at any time. If it is withdrawn and if in the meantime the data have been disclosed to third parties, the withdrawal is announced to them by the provider. The provider of a public network or publicly available electronic communications services is not permitted to depend the provision of

[6] Par. 5 of art. 4 was replaced as above by art. 170 of law 4070/2012 (Official Gazette A' 82/10.4.2012).
[7] Article 5 was replaced as above by art. 171 of law 4070/2012 (Official Gazette A' 82/10.4.2012).

these services to the subscriber or user on his/her consent to the processing of these data for other purposes than those serving directly the provision of the services that are related to the articles of the present law.

4. The processing of data that indicate the geographic location of the terminal equipment of a subscriber or user of a public network or publicly available electronic communications services for the provision of value added services is only permitted if these are rendered anonymous or with the explicit consent of the subscriber or user to the extent and for the duration necessary for the provision of an value added service. The service provider shall inform the user or subscriber, prior to obtaining his/her consent, about the type of data which will be processed, 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. The consent can be withdrawn at any time. Users or subscribers shall be given the possibility during each connection to the network or communication transmission, to withdraw temporarily their consent for the processing of traffic data using simple means and free of charge.
5. Exceptionally, location data processing by the providers of a public communications network or publicly available electronic communications service is permitted without the subscriber's or user's prior consent, in order to provide to the competent authorities dealing with emergency calls, including law enforcement agencies, ambulance services and fire brigades, the information necessary for the localization of the caller and only for this specific purpose. 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 Ensuring the Secrecy of Communications (ADAE).
6. Paragraphs 1 and 2 of the present article do not apply when the National Telecommunications and Postal Services Committee (EETT) is informed by the interested persons about the traffic data, for the purpose of resolving disputes relating mainly to interconnection or payment, according to provisions of effective legislation."[8]

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 last three 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,

[8] Article 6 was replaced as above by art. 171, par. 2 of law 4070/2012 ((Official Gazette A' 82/10.4.2012).

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 the 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 complementary personal data.
3. Subscribers shall be given the option not to be included in a print 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 included 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 complementary data.

Article 11
Unsolicited communications

1. "The use of automated calling systems [9] 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 with human intervention (calls) for the above purposes must not be performed, if the subscriber has stated to the provider of the publicly available electronic communications service that he/she does not wish to accept such communications in general."[10] The provider must enter these statements in a special subscriber directory, which shall be at the subscriber's disposal, free of charge.

"3. The e-mail contact details that have been lawfully obtained in the context of the sale of a product or a service or other transaction can be used for direct marketing of similar products or services by the supplier or the fulfilment of similar purposes, even when the recipient of the message has not given his/her prior consent, provided that he/she is clearly and distinctly given the opportunity to object, in an easy manner and free of charge, to such collection and use of electronic contact details when they are collected and on the occasion of each message in case the user has not initially refused such use.

4. The practice of sending e-mail messages for purposes of direct marketing of goods and services, as well as any kind of commercial purposes, shall be prohibited, when the identity of the sender or the person on whose behalf the message is sent, is not mentioned in a clear and explicit manner neither is a valid address to which the recipient can request the termination of such communications, or when it violates article 5 of P.D. 131/2003 (GGB 116A), as effective, or when the recipients are encouraged to visit webpages that violate the obligations deriving from the present article."[11]

"5. The providers of electronic communications services are obliged to take the suitable measures that are defined by a common act of DPA and ADAE for the prevention of unsolicited communications. From the provider of publicly available electronic communications services, who by negligence violated this obligation as well as the obligation that is foreseen in section b of paragraph 2, the recipients of unsolicited communications, hold their right to demand compensation for any property damage or pecuniary compensation for moral damage. Provision of article 14 paragraph 2 of the present law applies to the pecuniary compensation due to moral damage. The provider of electronic communications services is not obliged to provide compensation and take measures so that the breach doesn't occur again in the future if he/she proves that he/she is not liable for negligence.

6. Apart from compensation pursuant to article 14 of present law, the recipients of unsolicited communications as well as the providers of publicly available communications services by virtue of the procedure of article 14 par. 3 of present law have the right to demand from anyone that violates the aforementioned obligations that are stipulated in paragraphs 1-4 of the present article, not to repeat the breach in the future under the threat of pecuniary penalty."[12]

7. The above regulations also apply to subscribers who are legal entities.[13]

"8. DPA is appointed as the competent authority for the implementation of Regulation *(*EC*)* No 2006/2004 of the European Parliament and of the Council (EE L 364. 9.12.2004) in the sector of unsolicited communications. Regarding all the rest JMD (Joint Ministerial Decision) Z1-827/2006 (B' 1086 9.8.2006) applies, as effective."[14]

Article 12
"Security of Processing"[15]

1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services and the security of the public electronic communications network. 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, taking into account state of the art technical capabilities and the cost of their application.
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. If 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.

---

[9] The words "with or" shall be deleted from September 1st 2011 by virtue of art. 16 par. 1 of law 3917/2011 (Official Gazette A' 22/21.2.2011).

[10] The first section of par. 2 shall be replaced as above from September 1st 2011 by virtue of art. 16 par. 1 of law 3917/2011 (Official Gazette A' 22/21.2.2011).

[11] Paragraphs 3 and 4 were replaced as above with art. 172, par. 1 of law 4070/2012 ((Official Gazette A' 82/10.4.2012).

[12] Paragraphs 5 and 6 were added as above with art. 172 par. 2 of law 4070/2012 ((Official Gazette A' 82/10.4.2012).

[13] Paragraph 5 was renumbered to par 7 with art.172 par. 3 of law 4070/2012 ((Official Gazette A' 82/10.4.2012).

[14] Par. 8 was added as above with art. 172, par. 4 of law 4070/2012 ((Official Gazette A' 82/10.4.2012).

[15] The title of article 12 was replaced as above with art. 173, par. 1 of law 4070/2012 (Official Gazette A' 82/10.4.2012).

"3. Subject to article 10 of law 2472/1997, as effective, by the measures of the present article at least: a) it is ensured that only authorized personnel and for lawfully approved purposes shall have access to personal data, b) the stored or transferred personal data are protected against accidental or unlawful destruction, accidental loss or alteration and unauthorized or unlawful processing, including storage, access or disclosure and c) the application of security policy in relation to the processing of personal data is safeguarded. Relevant special provisions and regulations of Independent Authorities continue to apply.
4. The competent authorities issue recommendations for best practices about the security level that must be reached with the measures of the previous paragraphs.
5. In case of a personal data breach, the provider of publicly available electronic communications services notifies ADAE and DPA of the breach without undue delay. The notification to the competent authorities includes at least a description of the nature of the personal data breach and the contact points from which further information can be obtained. Moreover, the consequences of the breach are described and the measures that were suggested or taken by the provider to deal with the breach.
6. When the personal data breach may have unpropitious consequences to the personal data or the private life of the subscriber or other person, the provider notifies without undue delay the affected subscriber or the affected person. The notification of the previous section includes at least description of the nature of the personal data breach and the contact points from which further information can be obtained as well as recommendations that can limit potential unfavourable results from the personal data breach.
7. The notification of the affected subscriber or affected person of the personal data breach is not necessary if the provider has proved to the competent authorities in a satisfactory manner that he/she has applied the appropriate technical security measures and that these measures were applied for the data related to the security breach. These measures for technological protection must at least include secure data encryption so that unauthorized access is not possible. If the provider has not provided notification, according to paragraph 6 of present article, the competent authorities after examining the possible unpropitious consequences from the breach can ask him/her to do so.
8. With a joint act DPA and ADAE can issue guidelines on the circumstances under which the notification of the personal data breach is required from the provider, the format of this notification and the way according to which this notification must be done.
9. The providers that provide publicly available electronic communications services keep a file with personal data breaches that includes the description of relevant incidents, their results, corrective actions which they undertook, with sufficient data so that the competent authorities will be able to verify that they have complied with the provisions of the present article. This file includes only information that is necessary for this purpose.
10. For the handling of the personal data breaches pursuant to the provisions of the present article, the competent authorities notify each other mutually for the measures that they intend to take."[16]
11. 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 of the provider's electronic communications services or the provision of a value added service, and must be restricted to what is necessary for the purposes of such activities.[17]

Article 13
Competences of the Personal 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 Personal 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 Personal Data Protection Authority or ex officio.
4. In cases of breach of articles 1 to 17 of the present law, the application of which falls within the jurisdiction of the Personal Data Protection Authority, this imposes the administrative penalties provided by art. 21 of law 2472/1997. In cases of breach of the present law, the application of which 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 Personal 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

[16] Paragraphs 3-10 were added as above with art. 173 par. 2 of law 4070/2012 (Official Gazette A' 82/10.4.2012).
[17] Par. 3 was renumbered to par. 11 as above with art. 173 of law 4070/2012 (Official Gazette A' 82/10.4.2012).

electronic communications services must be forwarded to the National Telecommunications and Postal Services Committee (EETT).

5. A joint act by the Personal 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 Personal 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 Personal 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.
When 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 (GGB 287 A) is annulled when the present comes into force.

CHAPTER TWO

Modification of law 2472/1997 (GGB 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 an association or trade-union, health, social welfare and sexual life as well as criminal charges or convictions and membership to a society relating to the above.

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

e) "Personal Data File" ("File") shall mean any organised set of personal data which are accessible based on these specific criteria.

Article 18

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 the European Economic Area 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:
“Compliance with the previous paragraph is the Controller’s responsibility. 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 legal interests of thirds parties, if they are physically or legally incapable of giving their 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 processing is carried out by doctors or other persons rendering medical services and relates to medical data, 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 processing is carried out by lawyers, notaries, unpaid land registrars and court officers or associations of said parties, and relates to the provision of legal services to their clients, provided that the Controller and the

association members 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:
a. to states of the European Union
b. to a state non member of the European Union, only following a permit granted by the providing Authority, which may grant such permit only if it deems that the country in question ensures 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. The Authority's permit is not required if the European Committee has opined, under the procedure of art. 31, par. 2 of Directive 95/46/EC by the European Parliament and Council of the 24th October 1995, that said country guarantees a satisfactory level of protection, in the sense of par. 2 of rt. 25 of the above 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 them 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 point 5 of paragraph 2 art. 9 of law 2472/1997:
"The Controller offers adequate guarantees for the protection of personal data of the subjects and the exercise of their relevant rights, when the guarantees arise from contractual clauses, according to the present law. No permit is required if the European Commission has decided, according to art. 26, paragraph 4 of Directive 95/46/EC that certain contractual clauses offer adequate guarantees 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 licences it issues in implementation of paragraph 2, point 6."

Article 25

1. Point 3 of paragraph 3 of art. 10 of law 2472/1997 is replaced as follows:
"Without prejudice to any other provisions, the Authority shall issue or offer regulatory acts, in accordance with art. 19, par 1i, as to the level of security of data, IT and communication infrastructure, as well as on the protection measures necessary for each category of processing and data in view of technological developments in the field of privacy protection".

Article 26

The following cases are added to par. 2, art. 12 of law 2472/1997. These are numbered as follows:
"e. Per case, the correction, deletion or locking of data whose processing does not comply with the present law, in particular due to the imperfect or inaccurate nature of the data, and
f. the disclosure to third parties, who have been notified of the data, of any correction, deletion or locking executed in accordance to case e, if this is possible or does not entail extraordinary effort".

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 it shall inspect the technological infrastructure and other automated or non-automated means supporting the data processing. 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 complaints by data subjects relating to the implementation of the law and the protection of their 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 may archive any applications or complaints that are deemed groundless or self-evidently vague or are submitted unduly or anonymously. The Authority shall advise the data subjects and applicants as to its actions."

Article 29

Case o is added after case n in paragraph 1 of art. 19 of law 2472/1997:
"o. The national division of the Schengen Information System executes independent inspections, in accordance with art. 114, par. 1 of the Schengen Treaty Implementation Agreement (law 2514/1997 GGB 140A), the competences of the national supervisory authority provided in art. 23 of the EUROPOL Treaty (law 2605/1998 GGB 88 A) and the competences of the national supervisory authority provided in art. 17 of the Treaty on the use of IT in the customs sector (law 2706/1999 GGB 77A), as well as the supervisory competences arising from any other 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