The legal framework of personal data e-processing in the digital environment in Greece

By Konstantina G. Arkouli

1. Introduction

The digital networks are a significant human achievement and play a major role in our lives. Especially regarding the internet, we should point out that it is thought of as the threshold of a new era in the field of digital networks, on the grounds that its outbreak reversed the traditional communication framework.

The internet as well as the telecommunication networks have the following special characteristics: a. the contribution of subscribers' or users' personal data such as name, surname, telephone number, e-mail address etc to the network service provider, is mostly a precondition for entry to them[1], and b. the processing of specific personal data by the network service provider is inevitable with reference to the purposes of the conveyance of a communication, the subscriber billing and the interconnection payments. This fact in combination with the potentialities that are placed at human's disposal by the modern technological means makes it easy for administrators of digital networks or third parties, who are instigated by base motives (curiosity, speculation etc), to process illegally the aforementioned personal data[2].

The numerous menaces of infringement upon the private sphere of users or subscribers of digital networks (for instance phishing, pharming, tapping, intervention or surveillance of communications, hacking, packet-sniffing, spamming, formation of files with *"digital profiles"* of users or subscribers of electronic communications services etc), which arise from the technological evolution and the rapid development of digital networks, show the dire necessity of outlining clear and articulate rules for the protection of privacy in the digital environment. In this paper, we will present the legal framework of the personal data processing in the field of electronic communications according to the Law No. 3471/2006, which brings into force the dictates of the e-privacy Directive (Directive 2002/58/EC) in the Greek law and order. Especially, we will focus on the principles of personal data e-processing and the rules about the confidentiality of the communications in the digital networks and about unsolicited electronic communications, which are provided in the aforementioned Law.

2. Personal data and their categories in electronic communications

Personal data is any piece of personal information – even insignificant – which concerns an identified or identifiable person (e.g. name, surname, occupation, age, religion, political convictions, physical and moral well-being, private life, marital status etc). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors

specific to his physical, physiological, mental, economic, cultural or social identity[3]. If a piece of information is not related to an identified or identifiable person, it will not be called personal data[4]. The aforementioned definition of the term "personal data" is extremely broad[5] and is adopted by both the Directive 95/46/EC[6] and the Greek Law No. 2472/1997[7], which implements the dictates of the above Directive in the Greek legislation.

Concerning the personal data of users or subscribers of electronic communications, these are divided in the following categories, according to the Law No. 3471/2006:

a. *"Data in relation to the content of a communication"*[8] are the information, which are exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service with the purpose of the achievement of a communication, such as the content of a telephone conversation, a text message (fax, sms, e-mail etc) or a message with multimedia content (mms).

b. *"External data of a communication"* are the information that specify the circumstances, which individualize a communication[9], such as name, surname and telephone number or e-mail address of the parties, duration of a call, static IP address[10] etc. The *"external data of a communication"* are further categorized as follows:

1. *'Traffic data'*[11] means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof. Traffic data are particularly telephone number, address, location data, date, exact start time, exact end time and duration of a communication, information related to the protocol and the routing of a communication and billing data.
2. *'Location data'*[12] means 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. They may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of the travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded[13].

3. The scope of the Law No. 3471/2006

The first chapter (articles 1-17) of the Law No. 3471/2006 contains the provisions, which bring into force the dictates of the e-privacy Directive in the Greek law and order. The aforementioned articles apply to the processing of personal data and the protection of privacy in connection with the provision of publicly available electronic communications services in public communications networks. On the contrary, the general provisions of the Law No. 2472/1997 are applicable to the personal data processing that is carried out in connection with services provided by means of an intercommunication system of a company, since the case in question is beyond the scope of the Law No. 3471/2006.[14] So, if a network operates not only as a public communications network but also as an intercommunication system, the public communications network is governed by the provisions of the Law No. 3471/2006

and the intercommunication system is governed by the provisions of the Law No. 2472/1997.[15]

Regarding the subjective scope of the Law No. 3471/2006, it concerns not only individuals, but also legal entities. Though the protection of the *"private sphere"* of legal entities finds its basis in the article 9A of the Greek Constitution[16], the Law No. 3471/2006 is the one and only Greek Law about personal data protection, which provides directly for protection of the legitimate interests of subscribers who are legal entities[17]. This legal regulation complies with the e-privacy Directive[18] and answers practical purposes, which are summarized to the predicament of the providers of electronic communications services to process in a different way the personal data in view of whether they concern individuals or legal entities.[19]

4. The dictates of the Law No. 3471/2006 about personal data e-processing

a. Personal data processing principles in the publicly available electronic communications services

The keynote principles, which are provided by the Law No. 2472/1997 for the protection of personal data and privacy can govern the personal data processing in the field of electronic communications as well, on condition that they are modified appropriately. Therefore, in the digital environment the principle of lawful method of data collection[20] dictates that the personal data of electronic communications' users or subscribers should be collected fairly and lawfully and the principle of scope[21] provides that these data should be collected for specified, explicit and legitimate purposes and should not be further processed in a way incompatible with those purposes[22]. The aforementioned data should, also, be accurate, true, and –where necessary– kept up to date, according to the principle of accuracy[23]. Additionally, the Law No. 3471/2006 restates the principle of necessity, particularizes the principle of finite data retention duration and specifies the features of the data subject's consent to the processing of his/her personal data in the digital networks[24], as follows:

i. Principle of necessity

According to the principle of necessity, which is formulated in the Law No. 2472/1997, the personal data should be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.[25] Virtually, this principle is a specialization of the principle of proportionality.[26]

The principle of necessity of personal data processing occurs also in the Law No. 3471/2006 in a harsher phrasing.[27] Under this principle, personal data processing should be restricted to the extent that is absolutely necessary for the sort and the purpose of the processing[28]. Moreover, the providers of publicly available electronic communications services must take the appropriate technical measures and must

design and select the appropriate information systems in order to process the absolutely necessary personal data.[29]

We should, also, point out that the article 5 § 7 of the Law No. 3471/2006, as it was amended by the article 8 of the Law No. 3783/2009, obliges the providers of publicly available electronic communications services to render *the payment* for these services possible anonymously or pseudonymously, if it is technically feasible (e.g. with a prepaid card[30] for a specific duration of calls). Nevertheless, concerning *the use* of these services, the article 3 § 1 of the Law No. 3783/2009 provides that the users or subscribers must state solemnly the personal data, which are mentioned to the article 2 § 4 of the aforementioned Law[31], to the providers of publicly available electronic communications services. This legislative regulation aims at the protection of national security and the prevention, investigation, detection and prosecution of criminal offences, terroristic actions and organized crime by the prosecuting authorities.[32] It is a fact that anonymity in the field of electronic communications contributes to the protection of users' and subscribers' right to informational self-determination.[33] However, the undoubtedly respectable right to anonymity should not give rise to the impunity of criminal offenders.[34]

ii. Principle of finite data retention duration

According to the Law No. 2472/1997, personal data must be kept in a form, which renders the identification of data subjects possible up to the end of the period that is necessary for the purposes for which the data were collected or for which they are further processed.[35] This principle of finite data retention duration is further specified in the Law No. 3471/2006. So, subscribers' or users' traffic data, which are being processed and stored by the provider of a publicly available communications service, must be erased or made anonymous when it is no longer needed for the purpose of the processing.[36] Consequently, traffic data processing for the purpose of the conveyance of a communication is permissible only up to the end of each communication[37] and traffic data processing for the purposes of subscriber billing and interconnection payments is permissible only up to the end of the period during which the bill may be challenged lawfully or payment may be pursued[38], namely for the fulfillment of the contract[39]. As to location data, their processing is permissible to the extent and for the duration necessary for the provision of a value added service on condition that they are made anonymous with the appropriate codification or the service providers obtain the user's or subscriber's consent to the processing, after informing them about the type of location data which will be processed, about the purposes and duration of processing and about the eventual transmission of the data to a third party for the purpose of providing the value added service. In the latter case, users or subscribers should be given the possibility to withdraw their consent whenever and should have the opportunity to object to the processing of location data temporarily, free of charge and on the occasion of each connection to the network and each transmission of a communication.[40] Exceptionally, location data processing is permitted without the user's or subscriber's consent for the purpose of facing an emergency case.[41]

However, it must be stressed that the Law No. 3917/2011, which brings into force the regulations of the Data Retention Directive (Directive 2006/24/EC) in the

Greek law and order, dictates that the providers of publicly available electronic communications services or of a public communications network must retain the external data of an electronic communication for a period of twelve (12) months from the date of the communication to the extent that those data are generated or processed by them (the providers) within their jurisdiction in the process of supplying the communications services concerned[42]. So, the above recent Law redefines the retention period of the external data of an electronic communication by stretching the Law No. 3471/2006, and renders access to these data possible for the national authorities for the purposes of investigation, detection and prosecution of serious crimes[43]. The result of this recent legislative regulation is the dwindling of the protection, which the Law No. 3471/2006 provides in relation to the aforementioned data.[44]

iii. Users' or subscribers' consent as a prerequisite for lawful processing of their personal data

Users or subscribers of electronic communications services are mostly ignorant of the fact that, when they browse the web, they make legal transactions, such as consent to their personal data processing.[45] This consent leads to a shrinkage of users' and subscribers' private sphere[46] and is usually given in return for the provision of free information in the internet[47]. If the data subject does not consent to the processing of his/her personal data, his/her access to the information superhighways is not feasible.[48]

Consent is any freely given, explicit, specific and informed indication of wishes by which the data subject signifies his agreement to the processing of his personal data.[49] It is a unilateral legal transaction[50] that is addressed to the data controller, who is mostly the provider of publicly available electronic communications services. Data subject's consent has the following special characteristics:

a. It must be given freely. So, the user or subscriber must be able to decide on whether he will give his consent or not. At all events, consent must not be given under conditions of mental or physical violence[51], deception, fraud or threat, and must not contravene the statute and moral law[52].

b. It must be explicit and unambiguous on the grounds that it is of major importance for personal data protection.[53] Tacit consent is not valid.[54]

c. It must be specific, namely it must be given for a specific purpose and it must not cover in advance any future processing.[55] So, if the users or subscribers give their consent for any processing of their personal data without restrictions for the data retention period, the type of processing and the recipients to whom the data might be disclosed, this consent is not valid.[56]

d. Data controller is obliged to provide the user or subscriber with clear information about the categories of personal data, the purpose of the processing and the recipients or categories of recipients to whom the data might be disclosed as well.[57] The user or subscriber must, also, be informed about the name and the address of the controller and of his representative and the proposed transfers of data to third countries[58]. The notification must be easily comprehensible, true, clear and complete, namely must contain both positive and negative effects of the

processing.[59] Usually, the above information are included to the text of Privacy Policy of the website of a provider of electronic communications services.[60] Consent, which is given without prior adequate notification, is void, because it does not provide guarantees for the free expression of the user's or subscriber's will.[61]

It must be stressed that, though the Directive 2002/58/EC makes no provision for compliance with legal formalities about the data subject's consent for his personal data processing[62], the article 5 § 3 of the Law No. 3471/2006 provides that user's or subscriber's consent to the processing of his/her personal data must be given either through a document, which bears the data subject's handwritten signature or by *"electronic means"*[63], namely through an electronic document. However, it is not required for the electronic document to bear the advanced electronic signature, which would equate an electronic document with a document that bears a handwritten signature.[64] So, consent may be given on-line by any proper means that guarantees the free and informed expression of user's or subscriber's will. Therefore, consent may be given electronically, even by ticking a box when browsing a website (mouse-click consent).[65] At all events, the user's and subscriber's consent must be embodied permanently in a stable storage device, so that it is easy of access to him/her[66] and the data controller will be able in the future to prove the receiving of the consent.[67] If data controller obtains consent without being observant to the abovementioned legal formalities, the consent is void, according to the article 159 of the Greek Civil Code.

We should, also, emphasize that consent must be given in writing, if personal data are disclosed to third parties[68]. Providers of publicly available electronic communications services are not supposed to be third parties, regarding the traffic data transmission to them by another corresponding provider with the sole purpose of billing of the services, on condition that the user or subscriber has been informed in writing before the drawing up of the agreement.[69]

Eventually, the data subject has the right to withdraw his consent.[70] The withdrawal of this consent is a unilateral legal transaction, which is addressed to the controller and, according to the article 164 of the Greek Civil Code, is subject to consent's legal formalities.[71] In advance renunciation of the user's or subscriber's right to withdraw his consent is void, because it amounts to a blank consent to the processing of his personal data for any purpose in the future.[72]

b. The protection of the confidentiality of communications in the digital networks

According to the article 4 § 1 of the Law No. 3471/2006, the use of electronic communications services, which are provided by means of a public communications network and publicly available electronic communications services, as well as the related traffic data and location data, are protected as confidential. Consequently, listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data and location data is prohibited[73], except from the cases that is permitted by the Greek legislation for the purposes of protection of national security or detection of serious crimes.

However, technical storage of data, which are necessary for the conveyance of a communication is permitted without prejudice to the principle of confidentiality.[74] Technical storage is, also, lawful, if it is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user, on condition that the subscriber or user concerned is provided with clear and comprehensive information about the purposes of the processing and is offered the right to refuse such processing by the data controller.[75]

It is of high importance that traffic data, which are necessary for the purposes of subscriber billing and interconnection payments, may be processed lawfully by the provider of electronic communications services without the subscriber's prior consent[76], just because it is required for the fulfillment of the contract[77]. Such processing is permissible only up to the end of the period during which the bill may be lawfully challenged or payment may be pursued[78], as the purpose of the processing is the proof of the subscriber's debt. For example, the provider of a mobile network keeps legally a record of the home addresses of his subscribers, because it is necessary for the billing of the services and the dispatch of the bill. However, in the case of prepaid mobile services the processing of these data is not a prerequisite for the fulfillment of the contract, because the price for the services is prepaid, when the user buys the card and, thereupon, there is no question of payment or the bill is beyond dispute.[79]

We should, also, mention that the digital networks and the mobile telecommunications networks offer to the called subscriber the possibility of presentation of the calling line identification before the beginning of a communication[80]. As an offset to this possibility the article 8 § 1 of the Law No. 3471/2006 dictates that the calling user should be able to prevent the presentation of the calling line identification on a per-call basis using a simple means and free of charge. The calling subscriber is offered this possibility on a per-line basis. However, the possibility of preventing the presentation of the calling line identification of incoming calls must not become an obstacle to the detection of malicious[81] or nuisance[82] calls or to the handling of emergency calls. Therefore, traffic data and location data of users and subscribers of publicly available electronic communications services may, also, be processed without their consent in the aforementioned cases.[83] Consequently, the providers of publicly available electronic communications services must take the appropriate technical measures in order to render it possible to override: a. the elimination of the presentation of calling line identification, on a temporary basis, upon application of a subscriber requesting the tracing of malicious or nuisance calls, and b. the elimination of the presentation of calling line identification and the temporary denial or absence of consent of a subscriber or user for the processing of location data, on a per-line basis for organizations dealing with emergency calls for the purpose of responding to such calls.[84]

Finally, regarding the recording of electronic communications and the related traffic data, it is permissible when it is 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 on condition that both parties give their "*informed consent*".[85] On the contrary, if the abovementioned recording takes place without the consent of the parties, it is a breach of confidentiality of the communications and, therefore, it is prohibited.

c. The unsolicited electronic communications

The unsolicited electronic communications, namely the processing of the users' or subscribers' traffic data -mostly without their prior consent- for the purposes of direct marketing of products or services, is very common nowadays. These unsolicited electronic communications are carried out by means of automated calling systems *with or without* human intervention, facsimile machines (fax), electronic mail or via mobile networks.

The Greek legislator regulates the unsolicited electronic communications for the purposes of direct marketing with the article 11 of the Law No. 3471/2006. According to this article, the unsolicited electronic communications for the purposes of direct marketing, which is carried out by the abovementioned ways, are permitted only in respect of subscribers who have given their prior consent. The same rule applies to individuals and legal entities as well.[86]

Exceptionally, if an individual or legal entity obtains from its customers their electronic contact details, in the context of the sale of a product or a service, the same individual or legal entity may use these electronic contact details for direct marketing of its own similar products or services, on condition that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of their electronic contact details and on the occasion of each message in case the customer has not initially refused such use.[87] In addition, the practice of sending electronic mail for the purpose of direct marketing 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 request the cessation of such communications, is prohibited.[88]

We should, also, mention that the article 11 § 2 of the Law No. 3471/2006 regulates each provider of publicly available electronic communications services to keep an e-Robinson register, in which all the declarations of subscribers, who do not desire to receive unsolicited electronic communications for the purpose of direct marketing, will be recorded free of charge. Everyone, who proceeds to such communications, must refer regularly to these e-Robinson registers and must not disturb the subscribers, who are enrolled to them.[89]

The abovementioned rules adopt the system of prior consent for all the unsolicited electronic communications *with or without* human intervention parallel to the duty of the providers of publicly available electronic communications services to keep the e-Robinson register. However, this legal regulation contravenes the article 13 of the Directive 2002/58/EC for the following reason: The first paragraph of this article dictates that the use of automated calling systems *without* human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be permitted in respect of subscribers, who have given their prior consent. However, regarding the cases of unsolicited electronic communications *with* human intervention, the third paragraph of the above article dictates that Member States shall take appropriate measures to ensure that they are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications, the choice between

these options to be determined by national legislation. So, the present regulation of the article 11 § 1 of the Law No. 3471/2006 renders ineffective the article 11 § 2 of the same Law, because at all events prior consent of the user or subscriber is essential so that the unsolicited electronic communications are lawful[90].

In order to remove this contradictory regulation, the Greek legislator has already instituted the article 16 of the recent Law No. 3917/2011, which amends the aforementioned rules and takes effect on 1.9.2011[91]. According to this amendment, the unsolicited electronic communications for the purposes of direct marketing which are carried out by means of automated calling systems *without* human intervention, facsimile machines (fax) and electronic mail are permitted only with the prior consent of the user or subscriber. On the contrary, the unsolicited electronic communications for the above purposes, which are carried out by means of automated calling systems *with* human intervention, are prohibited, if the subscriber has declared to the provider of a publicly available electronic communications service that he/she does not want to receive such calls.

5. Conclusion

The abovementioned regulations of the Law No. 3471/2006, as it is amended, specify the conditions under which the processing of the personal data of users or subscribers of electronic communications is lawful and legitimate. So, these regulations set clear and distinct limits to the personal data e-processing by virtue of the needs and risks arising from the rapid development of the digital networks and, therefore, function as precautionary measures of personal data protection in the digital environment. If the personal data e-processing does not meet the requirements of the above Law without prejudice to the Greek legislative regulations, which put aside the confidentiality of the electronic communications, as well as the related traffic data and location data, for the purposes of protection of public safety and detection of serious crimes, it is illegal and gives rise to legal claims on the side of the harmed user or subscriber of electronic communications services.

---

[1] See *K. Christodoulou* (2006), Protection of personality and contractual freedom in public available networks *(in Greek)*, pp. 55-56 · *K. Christodoulou* (2008), Epitome of Electronic Civil Law *(in Greek)*, p. 16.

[2] See *Ap. Georgiades*, Private law on the threshold of 21st century *(in Greek)*, Nomiko Vima 2001, 575 · *G. Kaminis*, Privacy in telecommunications: Constitutional protection and its implementation by the penal legislator and the courts *(in Greek)*, Nomiko Vima 1995, 508 · *G. Georgiades*, The Law No. 3471/2006 about the protection of privacy in electronic communications *(in Greek)*, Chronika Idiotikou Dikaiou 2007, 17.

[3] See article 2 (c) of the Law No. 2472/1997 and article 2 (a) of the Directive 95/46/EC.

[4] See *E. Alexandropoulou-Egyptiadou* (2007), Personal Data *(in Greek)*, pp. 33-34.

[5] See *L. Mitrou* (1998), Technology and personal data protection *(in Greek)*, in: Proceedings of the 7th Panhellenic Conference of Commercial Law – Topic: The adjustment of the modern technology in Commercial Law, p. 195.

[6] See Article 2 (a).

[7] See Article 2 (a).

[8] See *G. Georgiades*, The Law No. 3471/2006 about the protection of privacy in electronic communications *(in Greek)*, Chronika Idiotikou Dikaiou 2007, 22 · *Gr. Tsolias*, The telecommunication data in the light of privacy: Problems in view of the implementation of the

Directive 2002/58/EC *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 2004, 360 · *K. Christodoulou* (2008), Epitome of Electronic Civil Law *(in Greek)*, p. 17.

[9] See *Gr. Tsolias*, The telecommunication data in the light of privacy: Problems in view of the implementation of the Directive 2002/58/EC *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 2004, 360 · *Gr. Tsolias*, To a modern legal framework for the protection of privacy in telecommunications (Presentation and annotation of the provisions of the Presidential Decree No. 47/2005), Poiniki Dikaiosini 7/2005, 794 · *G. Georgiades*, The Law No. 3471/2006 about the protection of privacy in electronic communications *(in Greek)*, Chronika Idiotikou Dikaiou 2007, 22 · *K. Christodoulou* (2008), Epitome of Electronic Civil Law *(in Greek)*, pp. 16-17.

[10] A static IP Address is personal data, because it remains unchanged each time the subscriber connects to the internet and is unique world-wide. On the contrary, a dynamic IP address changes each time the subscriber connects to the internet or during the connection. So, it is not personal data, unless the administrator of the website is able to identify the user or subscriber by using the means at his disposal. See relatively *I. Igglezakis*, The protection of personal data in the Internet – Regulations of national and community Law *(in Greek)*, Episkopisi Emporikou Dikaiou 2002, 684 · *A. Fragouli*, Are IP addresses personal data and which are the consequences?, Dikaio Meson Enimerosis & Epikoinonias 2/2008, 198 · *T. E. Synodinou* (2008), Intellectual Property and new technologies – The relation between user – creator, p. 286.

[11] See article 2 (3) of the Law No. 3471/2006 and article 2 (b) of the Directive 2002/58/EC.

[12] See article 2 (4) of the Law No. 3471/2006 and article 2 (c) of the Directive 2002/58/EC.

[13] See the 14th recital of the preamble of the Directive 2002/58/EC.

[14] See article 3 § 1 of the Law No. 3471/2006.

[15] Compare to *V. Tountopoulos*, Protection of personal data in the field of telecommunications – The implementation of the Directive 97/66 in the Greek legislation *(in Greek*), Dikaio Epixeiriseon & Etaireion 5/2000, 477.

[16] See *K. Christodoulou* (2006), Protection of personality and contractual freedom in public available networks *(in Greek)*, p. 102.
The article 9A of the Greek Constitution provides that "*Everyone* has the right of protection from the collection, processing and use, especially by electronic means, of his personal data, as specified by the Law."

[17] See *E.Papakonstantinou*, Comment for the Law No. 3471/2006 *(in Greek*), Efimerida Dioikitikou Dikaiou 4/2006, 444.

[18] See article 1 § 2 of the Directive 2002/58/EC.

[19] See *I. Igglezakis* (2006), Introduction to the law of informatics *(in Greek*), pp. 197-198 · *I. Igglezakis* (2008), Law of Informatics *(in Greek*), p. 256.

[20] See *P. Armamentos/ V. Sotiropoulos* (2005), Personal Data – Commentary of the Law No. 2472/1997 *(in Greek)*, p. 115. See, also, article 4 § 1 (a) of the Law No. 2472/1997 and article 6 § 1 (a) of the Directive 95/46/EC.

[21] See *P. Armamentos/ V. Sotiropoulos* (2005), Personal Data – Commentary of the Law No. 2472/1997 *(in Greek)*, p. 117.

[22] See article 4 § 1 (a) of the Law No. 2472/1997 and article 6 § 1 (b) of the Directive 95/46/EC.

[23] See *P. Armamentos/ V. Sotiropoulos* (2005), Personal Data – Commentary of the Law No. 2472/1997 *(in Greek)*, p. 130. See, also, article 4 § 1 (c) of the Law No. 2472/1997 and article 6 § 1 (d) of the Directive 95/46/EC.

[24] See the preamble of the Law No. 3471/2006 in the legal database www.dsanet.gr.

[25] See article 4 § 1 (b) of the Law No. 2472/1997 and article 6 § 1 (c) of the Directive 95/46/EC.

[26] See *P. Armamentos/ V. Sotiropoulos* (2005), Personal Data – Commentary of the Law No. 2472/1997 *(in Greek)*, p. 123.

[27] Compare to *V. Tountopoulos*, Protection of personal data in the field of telecommunications – The implementation of the Directive 97/66 in the Greek legislation *(in Greek*), Dikaio Epixeiriseon & Etaireion 5/2000, 479.

[28] See article 5 § 1 of the Law No. 3471/2006.

[29] See article 5 § 6 of the Law No. 3471/2006.

[30] According to the 13th recital of the preamble of the Directive 2002/58/EC, prepaid cards are considered as a contract.

[31] An individual must state his name, surname, father's name, place and date of birth and taxpayer's identification number to the network service providers and deposit to them a copy of his identity card. Respectively, a legal entity must state its firm, the address of its central offices, its taxpayer's identification number, as well as the name, surname and father's name of its legal representative.

[32] See the preamble of the Law No. 3783/2009 in the legal database www.dsanet.gr.
[33] See *Gr. Lazarakos,* Anonymity and Internet *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 2/2005, 199.
[34] See *M. Stathopoulos,* The use of personal data and the struggle between the rights of their controllers and the rights of their data subjects *(in Greek)*, Nomiko Vima 2000, 9 · *Gr. Lazarakos,* Anonymity and Internet *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 2/2005, 199.
[35] See article 4 § 1 (d) of the Law No. 2472/1997.
[36] See article 6 § 1 of the Law No. 3471/2006 and article 6 § 1 of the Directive 2002/58/EC.
[37] See articles 4 § 4 and 6 § 1 of the Law No. 3471/2006. See, also, articles 5 § 1 and 6 § 1 of the Directive 2002/58/EC.
[38] See article 6 § 2 of the Law No. 3471/2006 and article 6 § 2 of the Directive 2002/58/EC.
[39] See article 5 § 2 (b) of the Law No. 3471/2006.
[40] See article 6 § 3 of the Law No. 3471/2006 and article 9 §§ 1-2 of the Directive 2002/58/EC.
[41] See article 6 § 4 of the Law No. 3471/2006 and article 10 of the Directive 2002/58/EC.
[42] See articles 3 and 6 of the Law No. 3917/2011 and articles 3 and 6 of the Directive 2006/24/EC. The obligation to retain the external data of an electronic communication includes the retention of these data relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data), by the providers of publicly available electronic communications services or of a public communications network in the process of supplying the communication services concerned.
[43] See article 4 of the Law No. 3917/2011 and article 4 of the Directive 2006/24/EC.
[44] Compare to *I. Igglezakis* (2008), Law of Informatics *(in Greek*), p. 265.
[45] See *G. Georgiades* (2003), The contracting of an agreement via Internet *(in Greek)*, pp. 29-30.
[46] See *G. Nouskalis* (2004), The penal protection of digital information *(in Greek)*, in: Digital Technology and Law – Union of Jurists of Northern Greece, vol. 52, p. 164.
[47] See *G. Georgiades* (2003), The contracting of an agreement via Internet *(in Greek)*, p. 30 · *I. Igglezakis,* The protection of personal data in the Internet – Regulations of national and community Law *(in Greek)*, Episkopisi Emporikou Dikaiou 2002, 683.
[48] See *G. Nouskalis* (2004), The penal protection of digital information *(in Greek)*, in: Digital Technology and Law – Union of Jurists of Northern Greece vol. 52, p. 164.
[49] See article 2 of the Law No. 2472/1997 and article 5 §§ 2-4 of the Law No. 3471/2006.
[50] See *F. Doris,* in: Civil Code *Georgiades/Stathopoulos (in Greek*), art. 236, section 10.
[51] See *G. Georgiades,* The Law No. 3471/2006 about the protection of privacy in electronic communications *(in Greek)*, Chronika Idiotikou Dikaiou 2007, 22.
[52] See *K. Christodoulou*, To a re-examination of the meaning of the legal transaction? The paradigm of data subject's consent to his personal data processing *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 3/2005, 359 · *E. Alexandropoulou-Egyptiadou* (2007), Personal Data *(in Greek)*, p. 45.
[53] Compare to *V. Tountopoulos,* Protection of personal in the field of telecommunications – The implementation of the Directive 97/66 in the Greek legislation *(in Greek*), Dikaio Epixeiriseon & Etaireion 5/2000, 479.
[54] Compare to *I. Igglezakis* (2004), Sensitive personal data *(in Greek*), p. 218.
[55] See *K. Christodoulou*, To a re-examination of the meaning of the legal transaction? The paradigm of data subject's consent to his personal data processing *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 3/2005, 361 · *E. Alexandropoulou-Egyptiadou* (2007), Personal Data *(in Greek)*, p. 60.
[56] Compare to *I. Igglezakis* (2004), Sensitive personal data *(in Greek*), pp. 220 and 222.
[57] See article 5 § 2 of the Law No. 3471/2006.
[58] Compare to *I. Igglezakis* (2004), Sensitive personal data *(in Greek*), p. 220. See, also, article 2 of the Law No. 2472/1997.
[59] See *Gr. Lazarakos*, Creation of Websites and personal data protection *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 4/2005, 553-554.
[60] See *I. Igglezakis* (2004), Sensitive personal data *(in Greek*), p. 222.
[61] See *K. Christodoulou*, To a re-examination of the meaning of the legal transaction? The paradigm of data subject's consent to his personal data processing *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 3/2005, 358 · *I. Igglezakis* (2004), Sensitive personal data *(in Greek*), p. 220.
[62] See *K. Christodoulou* (2006), Protection of personality and contractual freedom in public available networks *(in Greek)*, p. 107.
[63] See *K. Christodoulou* (2006), Protection of personality and contractual freedom in public available networks *(in Greek)*, p. 104.

[64] See *K. Christodoulou* (2006), Protection of personality and contractual freedom in public available networks *(in Greek)*, p. 104.
[65] See the 17th recital of the preamble of the Directive 2002/58/EC. Also, see *Korn. Delouka-Igglesi*, Consumer's protection from the direct advertisement in the internet *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 4/2004, 496 · *An. Spiliotopoulou/I. Chochliouros*, Lawful interception of communications while ensuring individual's privacy *(in Greek)*, Nomiko Vima 2007, 1961. Referring to the term "mouse-click consent", it occurs in: *L. Mitrou* (2005), Self-regulation in the Cyberspace *(in Greek)*, in: *Th. K. Papachristou/ Ch. Vernardakis/ G. Theodosis/ If. Kamtsidou/ K. Manolakou/ L. Mitrou/ V. Papakonstantinou/ E. Rethimniotaki/ K. Stratilati/G. Tasopoulos*, Self- regulation, Law & Society in the 21st Century, vol. 9, p. 85.
[66] See article 5 § 3 of the Law No. 3471/2006.
[67] See *K. Christodoulou* (2006), Protection of personality and contractual freedom in public available networks *(in Greek)*, p. 105.
[68] For the meaning of the term "third party" see article 2 of the Law No. 2472/1997 and article 2 (f) of the Directive 95/46/EC.
[69] See article 5 § 5 of the Law No. 3471/2006.
[70] See article 5 § 3 of the Law No. 3471/2006.
[71] See *F. Doris*, in: Civil Code *Georgiades/Stathopoulos (in Greek*), art. 237, section 5.
[72] See *K. Christodoulou*, To a re-examination of the meaning of the legal transaction? The paradigm of data subject's consent to his personal data processing *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 3/2005, 363.
[73] See article 4 § 2 of the Law No. 3471/2006 and article 5 § 1 of the Directive 2002/58/EC.
[74] See article 4 § 4 of the Law No. 3471/2006 and article 5 § 1 of the Directive 2002/58/EC.
[75] See article 4 § 5 of the Law No. 3471/2006 and article 5 § 3 of the Directive 2002/58/EC.
[76] See article 6 § 2 of the Law No. 3471/2006 and article 6 § 2 of the Directive 2002/58/EC.
[77] See article 5 § 2 of the Law No. 3471/2006.
[78] See article 6 § 2 of the Law No. 3471/2006 and article 6 § 2 of the Directive 2002/58/EC.
[79] See *Gr. Tsolias*, Personal Data in the field of electronic communications and "reverse search" of them for the purpose of detection of very serious crimes – On the occasion of No. 19/2008 Decision of the Greek Data Protection Authority *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 2/2008, 178.
[80] See *L. Mitrou*, The new Directive 2002/58/EC for the protection of privacy in electronic communications, Dikaio Meson Enimerosis & Epikoinonias 3/2004, 374.
[81] Malicious call is the call, which poses a threat of violence/compulsion or other unlawful act or failure, insult, affront to sexual dignity or extortion. For the meaning of the term "malicious call" see article 2 of the act No. 2322/11.12.2006 of the Hellenic Authority for Communication Security and Privacy.
[82] Nuisance call is the call, which disturbs domestic peace and causes anxiety (e.g. silent and repeated calls). For the meaning of the term "nuisance call" see article 2 of the act No. 2322/11.12.2006 of the Hellenic Authority for Communication Security and Privacy.
[83] See article 8 § 7 of the Law No. 3471/2006.
[84] See article 8 § 7 of the Law No. 3471/2006 and article 10 of the Directive 2002/58/EC. The elimination of the presentation of calling line identification may be overridden: a. upon application of a subscriber requesting the tracing of malicious or nuisance calls, and b. for the purpose of dealing with emergency calls, under the requirements of the acts No. 2322/11.12.2006 and 2002/3.9.2008 of the Hellenic Authority for Communication Security and Privacy.
[85] See article 4 § 3 of the Law No. 3471/2006 and article 5 § 2 of the Directive 2002/58/EC.
[86] In relation to these regulations see article 11 §§ 1 and 5 of the Law No. 3471/2006.
[87] See article 11 § 3 of the Law No. 3471/2006 and article 13 § 2 of the Directive 2002/58/EC.
[88] See article 11 § 4 of the Law No. 3471/2006 and article 13 § 4 of the Directive 2002/58/EC.
[89] See *Korn. Delouka-Igglesi*, Consumer's protection from the direct advertisement in the internet *(in Greek)*, Dikaio Meson Enimerosis & Epikoinonias 4/2004, 496.
[90] See the preamble of the Law No. 3917/2011 in the website http://www.ministryofjustice.gr/site/LinkClick.aspx?fileticket=In68q5jjdW0%3d&tabid=132.
[91] See article 16 § 3 of the Law No. 3917/2011.