Data Protection & Privacy

In 31 jurisdictions worldwide

Contributing editor
Rosemary P Jay

2015

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2015

Contributing editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
George Ingledew
george.ingledew@lbresearch.com

Alan Lee
alan.lee@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2012
Third edition
ISSN 2051-1280

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Greece

George Ballas and Theodore Konstantakopoulos
Ballas, Pelecanos & Associates LPC

Law and the regulatory authority

1 Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

The legislative framework for the protection of personally identifiable information (PII) includes Data Protection Law 2472/1997 (Protection of Individuals with regard to the Processing of Personal Data) and Law 3471/2006 (Protection of personal data and privacy in the electronic telecommunications sector) implementing relevant EU data protection legislation (Directives 95/46/EC and 2002/58/EC). Moreover, Data Retention Directive 2006/24/EC has been implemented by Law 3917/2011.

The Greek legal framework also includes regulations and directives issued by the Hellenic Data Protection Authority (DPA), for instance, Directive 50/2001 on direct marketing and Directive 115/2001 on privacy at work.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the powers of the authority.

The Hellenic Data Protection Authority (DPA), a constitutionally consolidated independent authority, is responsible for overseeing the data protection law in Greece. The DPA issues regulatory acts (directives) for the purpose of a uniform application of the data protection legislation, publishes Guidelines, addresses recommendations and instructions to data controllers, grants permits for the collection and processing of sensitive PII and for the transborder flow of PII, imposes administrative sanctions and performs administrative audits.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

Breach of the provisions of the Data Protection Law 2472/1997 can lead to criminal penalties; penal sanctions include imprisonment up to 10 years and fine between €2,900 and €29,300. In practice and depending on the severity and the particular circumstances of the breach, the DPA can request a hearing and/or issue an order for compliance before pursuing criminal sanctions or imposing any administrative sanctions.

Scope

4 Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The provisions of Data Protection Law 2472/1997 do not apply to the processing of PII which is carried out: by a natural person in the course of a purely personal or household activity and by judicial and public prosecution authorities in the framework of the performance of their duties and for the purposes of investigation of crimes which are punished as felonies or misdemeanours with intent, including in particular crimes against life, against sexual freedom, crimes involving the economic exploitation of sexual life, crimes against personal freedom, against property, violations of legislation on drugs and crimes against minors.

5 Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

According to Data Protection Law 2472/1997, interception of communications and monitoring and surveillance of individuals is permitted only for the purposes of investigation of the crimes mentioned above (in question 4), further to a relevant order by the Public Prosecutor and provided that a serious danger to the public order and security is imminent. Other legislation (Law 2225/1994 and Presidential Decree 47/2005) regulate in detail the circumstances under which 'lifting of secrecy of communications' can be ordered and the procedures, time limits and technical and organisational safeguards that need to be followed. Electronic marketing is regulated by Law 3471/2006 (Protection of personal data and privacy in the electronic telecommunications sector).

6 Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas?

Laws and regulations that provide specific data protection rules for related areas include Law 3418/2005 (Medical Ethics Code) on health records, Article 5 of the Code of Administrative Procedure regulating access to public records, Law 3758/2009 on the operation of debt collection agencies and Law 4174/2013 on tax collection.

7 PII formats

What forms of PII are covered by the law?

All PII formats are covered by the provisions of the Data Protection Law 2472/1997.

8 Extraterritoriality

Is the reach of the law limited to data owners and data processors established or operating in the jurisdiction?

The Data Protection Law 2472/1997 applies when data processing is carried out by a data controller or data processor with a seat in Greece or by a data controller with no seat in the EU or European Economic Area (EEA), which for the purposes of processing PII, makes use of equipment, automated or otherwise, located in Greece, unless such equipment is used only for transit purposes.

9 Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide services to owners?

Data processing includes any operation or set of operations which is performed by public authorities or by a public law entity or a private law entity or an association or a natural person, with or without automatic means,

including the collection, recording, organisation, retention, storage, alteration, use, disclosure, transfer, interconnection, destruction or deletion of PII. Data processing can be performed either by a data controller (ie, the person who or entity which determines the purposes and means of processing of PII) and/or a data processor (ie, the person who or entity which processes PII on behalf and under the instructions of a data controller).

Legitimate processing of PII

10 Legitimate processing – grounds

Does the law require that the holding of PII be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

PII, in order to be lawfully processed (including storage), must be collected and processed lawfully for specific, explicit and legitimate purposes. Processing of PII is in principle permitted only when the individual (data subject) has provided his or her consent. Exceptions apply; for instance, when processing is necessary for the execution of a contract to which the data subject is party (provided that the individual has been properly informed), no consent is required, and when processing involves clients' or suppliers' PII, provided that such data are neither transferred nor disclosed to third parties.

11 Legitimate processing – types of data

Does the law impose more stringent rules for specific types of data?

The collection and processing of sensitive data is prohibited. The Data Protection Law 2472/1997 defines 'sensitive data' as data referring to racial or ethnic origin, health, sexual life and social welfare. Exceptionally, such processing may be permitted pursuant to a permit by the DPA, under specific conditions, eg, when the data subject has provided his or her written consent; when processing is carried out exclusively for research and scientific purposes, provided that anonymity is ensured and all necessary measures for the protection of the persons involved are taken; when processing is carried out by a public authority and it is necessary for the purposes of national security, protection of public health or tax enforcement or it pertains to the detection of offences.

Data handling responsibilities of owners of PII

12 Notification

Does the law require owners of PII to notify individuals whose data they hold? What must the notice contain and when must it be provided?

The data subject must be informed at least about the following: the identity of the data controller and its representative (if any), the purpose of the data processing, the recipients or the categories of recipients of such data and the existence of the rights to access and object.

13 Exemption from notification

When is notice not required?

The legal obligation to provide notice to a data subject may be lifted pursuant to a relevant decision by the DPA and provided that data processing is carried out for reasons of national security or for the detection of particularly serious crimes. Moreover, under specific circumstances, no notice is required when data collection and processing is carried out solely for journalistic purposes and refers to public figures.

14 Control of use

Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Individuals have the right to access the PII relating to them and being processed by the PII owners; the latter must answer in writing. Moreover, individuals have the right to object to the processing of PII relating to them and being processed by the PII owners. Such a objection must be addressed in writing to the PII owner and must include a request for a specific action, such as correction, temporary non-use, non-transfer or deletion. The PII owner must reply in writing to such a objection within 15 days.

15 Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PII?

PII, in order to be lawfully processed, must be: collected and processed lawfully for specific, explicit and legitimate purposes; adequate, relevant and not excessive in relation to the purposes for which they are processed at any given time; accurate and if required up to date; and retained for no longer than the period required for the purposes for which such data were collected and processed.

16 Amount and duration of data holding

Does the law restrict the amount of PII that may be held or the length of time it may be held?

According to the Data Protection Law 2472/1997, PII collected and processed must be adequate, relevant and not excessive in relation to the purposes for which they are collected and processed at any given time. The general principle is that retention period must not be longer than the period required for the purposes for which such data were collected and processed. However, sector-specific specific regulation provides for specific data retention requirements; for instance Law 3917/2011 (implementing Directive 2006/24/EC), applicable to providers of publicly available electronic communications services or of public communications networks, imposes data retention obligations for the purposes of the investigation, detection and prosecution of serious crimes (a restrictive list of which is included in Law 2225/1994). The length of said retention period is 12 months starting from the date of the communication.

17 Finality principle

Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

According to the Data Protection Law 2472/1997, PII must be collected and processed lawfully for specific, explicit and legitimate purposes and also be adequate, relevant and not excessive in relation to the purposes for which they are processed at any given time.

18 Use for new purposes

If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

The general principle is that PII may not be used incompatibly with the purposes for which said data was originally collected. New data processing purposes require relevant notice to the data subject; consent by the data subject could also be required. Regarding the exceptions to the obligation to obtain consent, please refer to answers to questions 10 and 11 and regarding the exceptions to provide notice to a data subject, please refer to the answer to question 13.

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

According to article 10 of Data Protection Law 2472/1997, the processing of personal data must be confidential. It must be carried out solely and exclusively by persons acting under the authority and instructions of the data owners (data controllers) and entities that process PII on their behalf (data processors). In order to carry out data processing the data owners must choose persons with professional qualifications that provide sufficient guarantees in respect of technical expertise and personal integrity in order to ensure such confidentiality. Further, data owners must implement appropriate organisational and technical measures to secure data and protect them against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data subject to processing. If data processing is carried out on behalf of the data owner by a third party, such assignment must necessarily be in writing and provide that said third party carries out such data processing pursuant to

the instructions of the data owner and that all above security obligations shall mutatis mutandis be borne by such third party.

Further, the DPA has issued the 1/2011 Directive on the use of video surveillance systems for the protection of people and property, according to which the Data Controller must implement technical measures that ensure data safety and access control to central CCTV management, storage and processing areas. Well-trained personnel must be employed, and 'privacy by design' tools and processes must be implemented (eg, 'privacy mask' function, encryption and access certification). In cases when management and operation of the CCTV system is outsourced to a third party (data processor) such assignment must in writing and in accordance with Data Protection Law 2472/1997. Moreover, the DPA has also issued the 1/2005 Directive with regard to the data deletion requirements, referring to specific 'secure' and liable deletion methods and procedures. Relevant also are the DPA Guidelines on Security Policy, Security Plan and Disaster Recovery and Contingency Plan.

Reference is also made to the 205/2013 Decision of the Hellenic Authority for Communication Security and Privacy (ADAE) (Regulation for the Safety and Integrity of Networks and Electronic Communications Services) applicable to the providers of public communication networks or public electronic communication services. Said regulation defines the technical and organisational measures that need to be implemented by the providers of public communication networks or public electronic communication services to ensure data security, including reference to business impact analysis, business continuity, penetration tests, vulnerability assessments, physical security, backups, power management, logical access controls, security zones, firewalls, VPNs, intrusion detection systems, event logging and security incident management.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

According to Law 4070/2012, providers of public communication networks or public electronic communication services must report to the National Telecommunications and Post Commission (EETT) any security breach 'which had a significant impact on the operation of the networks or the service'. Moreover, a notification obligation in case of PII breaches is imposed on all providers of publicly available electronic communications services (ISPs and other telecoms), which must notify both the Hellenic Authority for Communication Security and Privacy (ADAE) no later than 24 hours after the detection of the personal data breach and also customers about such breaches. ADAE has published an online notification form of incident of personal data breaches (in compliance with EU Regulation No. 611/2013 on the notification of personal data breaches).

Internal controls

21 Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

In the private sector the appointment of a data protection officer is not mandatory; appointment is considered, however, as best practice. On the other hand, for public sector entities offering e-governance services the appointment of a data protection officer is obligatory by virtue of Law 3979/2011, according to which the data protection officer is responsible for the implementation of technical and organisational measures to ensure compliance with the principles and obligations provided by the data privacy legislation and also for the drafting of a privacy and security policy and for the provision of data privacy policy training to employees and personnel.

Moreover, and as matter of best practice, a data protection officer is expected to have a detailed and up-to-date knowledge of the data collection and processing operations of the organisation. He or she should identify the scope, the purposes and the means of each data processing operation and he or she is also expected to maintain a list of all databases and files containing personal data. A data protection officer is expected to proactively identify policy issues, conduct internal reviews, draft internal reports and generally observe any legal data protection obligations.

22 Record keeping

Are owners of PII required to maintain any internal records or establish internal processes or documentation?

Article 10 of the Data Protection Law lays down the general principle on confidentiality and security of processing, according to which owners of PII must implement appropriate organisational and technical measures to secure data and protect them against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data in question. Maintenance of internal records, establishment of internal processes and documentation can be organisational measures aiming at data security.

Registration and notification

23 Registration

Are owners and processors of PII required to register with the supervisory authority? Are there any exemptions?

Data controllers must notify the DPA in writing about the establishment and operation of a file or the commencement of data processing; exceptions apply, for instance (inter alia):

- when processing is carried out exclusively for purposes relating directly to an employment relationship and it is necessary for the fulfilment of an obligation imposed by law or for the accomplishment of obligations arising from the aforementioned relationship, and upon prior information to the data subjects;
- when processing involves customers' or suppliers' PII, provided that such data are neither transferred nor disclosed to third parties; and
- when processing involves medical data and is carried out by doctors or other persons rendering medical services, provided that the data controller is bound by medical confidentiality or other obligation of professional secrecy, and the PII are neither transferred nor disclosed to third parties.

24 Formalities

What are the formalities for registration?

The data controller must notify the Authority in writing about the establishment and operation of a file or the commencement of data processing (no relevant fee is payable). Such notification must include:

- the data controller's name and contact details;
- the address where the file or the main hardware supporting the data processing is located;
- the data processing purposes;
- the categories of personal data that are being processed;
- the data processing time period; the recipients or the categories of recipients of the data;
- any data transfers outside Greece; and
- the basic properties of the IT system and the data safety measures in place.

Any change to or modification of the information included in such notification must be communicated in writing and without any undue delay by the data controller to the DPA.

25 Penalties

What are the penalties for a data owner or processor for failure to make or maintain an entry on the register?

Anyone who fails to notify the DPA about the establishment and operation of a PII file or proceeds with the interconnection of files without notifying the DPA can be punished with imprisonment for up to three years and a fine ranging from €2,953 to €14,765. The DPA can also impose administrative sanctions, which include a warning and a cessation order, fine ranging from €880 to €146,735, revocation of a permit and destruction of the data file.

26 Refusal of registration

On what grounds may the supervisory authority refuse to allow an entry on the register?

The DPA can refuse to allow an entry on the register if, based on the particulars of the data collection and processing, there is no legal obligation to file such notification with the DPA. Moreover, in case of missing information or when additional clarifications are required, the DPA will communicate a relevant request to the data controller.

27 Public access

Is the register publicly available? How can it be accessed?

The (physical) register is publicly available upon relevant request to DPA. An electronic version of the registry is expected within the following year.

28 Effect of registration

Does an entry on the register have any specific legal effect?

The entry on the register can be a prerequisite for legitimate data processing and consists of the fulfilment of such legal obligation of the data controller.

Transfer and disclosure of PII

29 Transfer of PII

How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The data controller can in principle outsource data processing services. For this purpose and according to Data Protection Law 2472/1997, the data controller must choose data processors with professional qualifications that provide sufficient guarantees in respect of the technical expertise and personal integrity in order to ensure data safety and confidentiality. The data controller must implement appropriate organisational and technical measures to secure data and protect them against accidental or unlawful destruction, accidental loss, alteration, unauthorised disclosure or access as well as any other form of unlawful processing. Such measures must ensure a level of security appropriate to the risks presented by processing and the nature of the data in question. Data processing agreements must be in writing and provide that the data processor carries out data processing only based on the instructions received by the data controller and that all above security obligations shall mutatis mutandis be borne by such data processor.

30 Restrictions on disclosure

Describe any specific restrictions on the disclosure of PII to other recipients.

Disclosure of PII to judicial and public prosecution authorities is not regulated by the Data Protection Law, provided that it take place in the framework of the performance of their duties and for the purposes of investigation of crimes which are punished as felonies or misdemeanours with intent.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The general rule is that transfer of PII is permitted within the member states of the EU/EEA and PII can only be transferred to countries outside the EU/EEA when an adequate level of protection is guaranteed. Data transfer to the US can be allowed either on the basis of a permit by the DPA, or on the basis of a Safe Harbor certificate/ EC Standard Contractual Clauses (with no need for a permit by the DPA).

According to article 9 of Law 2472/1997, the transfer of PII is permitted:

- for member states of the EU; or
- for a non-member of the EU on the basis of a permit granted by the DPA, if the DPA deems that the country in question guarantees an adequate level of protection.

A Permit by the DPA is not required if the European Commission has decided, on the basis of the process of article 31, paragraph 2 of Directive 95/46/EC of the Parliament and the Council of 24 October 1995, that the country in question guarantees an adequate level of protection, in the sense of Article 25 of the aforementioned Directive. The transfer of PII to a non-member state of the EU/EEA which does not ensure an adequate level of protection is exceptionally allowed only following a permit granted by the DPA, provided that specific conditions are met (data subject's consent, approved data transfer contractual clauses, etc). No permit is required when Standard Contractual Clauses or Binding Corporate Rules (BCRs) are in place.

32 Notification of transfer

Does transfer of PII require notification to or authorisation from a supervisory authority?

If the data controller is obliged to submit a notification with the DPA (on this, please refer to answer to question 23), such notification must include reference to data processors, recipients and categories of recipients of the PII. Authorisation (by permit) could be required under specific circumstances, for example if sensitive data are processed.

Moreover, transfer of PII outside the EU/EEA can require notification to the DPA. Authorisation (by permit) could be required depending on the country where the data recipient is located and also on the contractual basis of such transfer (for additional information on this, please refer to the answer to question 31).

33 Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Restrictions also apply to transfers to service providers and onward transfers outside the EU/EEA. For instance, in the case of data transfer from a data controller to a data processor located outside the EU/EEA on the basis of EC Standard Contractual Clauses (Model Clauses), article 11 of the Model Clauses (prior written consent of the data exporter is required) would be applicable for onwards transfers to sub-processors.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

Individuals have the right to access the PII relating to them and being processed by the PII owners; the latter must answer in writing. The obligation to provide access to data may be lifted pursuant to a relevant decision by the DPA, provided that data processing is carried out for reasons of national security or for the detection of particularly serious crimes.

35 Other rights

Do individuals have other substantive rights?

Individuals have the right to object to the processing of PII relating to them and being processed by the PII owners. Such objection must be addressed in writing to the PII owner and must include a request for a specific action, such as correction, temporary non-use, non-transfer or deletion. The PII owner must reply in writing to such objection within 15 days.

36 Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

A person or legal entity that, in breach of data protection law, causes actual damage to a data subject can be liable for damages. If non-pecuniary damage was caused, the actor can be liable for compensation for moral damage. The compensation payable for non-pecuniary damage caused in breach of Data Protection Law is set by law at the amount of at least €5,870, and such compensation will be awarded irrespective of any claim for damages.

37 Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Individuals (data subjects) can exercise their rights through both the judicial system and the DPA, the supervisory authority.

Update and trends

Hot topics gradually gaining attention by the DPA include the bring-your-own-device (BYOD) use of smart devices by employees and the implementation of Internet of Things (IoT) technologies.

The DPA is expected within the next year to publish Guidelines or a Directive on BYOD, which will address data privacy and safety considerations and suggest appropriate technical and organisational data safety measures.

While the implementation of IoT technologies has not, as of today, been officially and specifically regulated in Greece, geolocation and RFID technologies have been within the scope of the DPA's mission and work and also an issue of legal debate. The DPA has adopted the WP29 Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID applications and it has examined the issue of the use of geolocation technology for the localisation of individuals. The use of wireless machine-to-machine (M2M) technology has also been reviewed by the DPA within the context of 'eCall' (in-vehicle emergency call), a European Union initiative, with the purpose of bringing rapid assistance to motorists involved in a collision. Finally, the public health considerations associated with the implementation of IoT technologies, though not included in any type of legislative text, are currently a core element of the legal discussion on RFID technology.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

In the case of a decision issued by a PII owner which affects the data subject and which is based solely on automated processing of data and intended to evaluate data subject's personality and especially its performance at work, creditworthiness, reliability and general conduct, the data subject has the right to request from the competent court the immediate suspension or non-application of such decision.

Supervision

39 Judicial review

Can data owners appeal against orders of the supervisory authority to the courts?

Yes, data owners can appeal against orders of the supervisory authority to the competent courts.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

Anyone who fails to notify the DPA about the establishment and operation of a PII file, or proceeds with interconnection of files without notifying the DPA, can be punished with imprisonment up to three years and a fine ranging from €2,953 to €14,765. Anyone who maintains a file without a permit by the DPA (when required) or in breach of the terms and conditions mentioned in such permit can be punished with imprisonment up to five years and a fine ranging from €2,953 to €14,765. Anyone who unlawfully interferes in any way whatsoever with a PII file or illegally takes notice of, extracts, alters, affects in a harmful manner, destroys, processes, transfers, discloses, makes accessible to unauthorised persons or permits such persons to illegally record such data can be punished with imprisonment up to five years and a fine up to €29,530.

41 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

The EU Cookies Directive has been implemented in Greece by virtue of article 170 of Law 4070/2012, according to which the storage of information on or the access to information already stored on a device of a user is permitted only if the user has provided his informed consent. Such consent can be expressed by using the appropriate settings of a browser or other application. The above does not prevent any technical storage or access for the sole purpose of carrying out a transmission of a communication over an electronic communications network or any technical storage or access which is necessary for the provision of an information society service, which has been explicitly requested by the user.

Moreover, the DPA guidelines on cookies refers to exceptions where no consent is required (basically reproducing the WP Opinion 04/2012 on Cookie Consent Exemption); such are the cases of 'user-input' cookies, user-centric security cookies, multimedia player session cookies, authentication cookies, UI customisation cookies, load balancing session cookies and social plug-in content sharing cookies. Special reference is also made to 'web analytics' cookies and 'online advertising' cookies (first-party cookies and third-party cookies), which according to the guidelines are not included in the above exceptions and therefore prior consent is required. The DPA recognises though the need to further review and discuss the issue of 'web analytics' cookies. According to the DPA guidelines, a user-friendly mechanism to opt out must be in place.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Marketing by e-mail, fax and SMS requires the recipient's consent (opt in). An exception applies when contact details of the recipient have been lawfully obtained in the context of the sale of a product or a service. In such case e-mails and SMS can be sent for direct marketing of similar products or services even when the recipient of the message has not given his or her prior consent, provided that he or she is clearly and distinctly given the option to object, in an easy manner and free of charge, to such collection and use of electronic contact details.

Marketing by telephone (with human intervention) is permitted unless the recipient has opted out from such communication. However, direct marketing by telephone without human intervention (via automated calls) requires opt-in consent.

George Ballas **george.ballas@balpel.gr**
Theodore Konstantakopoulos **theodore.konstantakopoulos@balpel.gr**

10 Solonos Street
Kolonaki
106 73 Athens
Greece

Tel: +30 210 36 25 943
Fax: +30 210 36 47 925
www.ballas-pelecanos.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains and Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Government Investigations
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Ship Finance
Shipbuilding
Shipping
State Aid
Tax Controversy
Tax on Inbound Investment
Telecoms and Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Partner of the ABA Section of International Law