Assembleia da República (Assembly of the Republic)

Law


The Assembleia da República (Assembly of the Republic), under article 161 c) of the Constitution, hereby decrees as follows:

**Article 1**

**Subject-matter**

This law:

a) Introduces the first amendment to Law No 41/2004, of 18 August, which transposes into the national legal order Directive 2002/58/EC, of the European Parliament and of the Council, of 12 July, concerning the processing of personal data and the protection of privacy in the electronic communications sector;


**Article 2**

**Amendment to Law No 41/2004, of 18 August**

Articles 1, 2, 3, 5, 6, 7, 8, 14 and 15 of Law No 41/2004, of 18 August, are hereby amended to read as follows:

«Article 1

[...]


2 - This law shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks, including public communications networks supporting data collection and identification devices, specifying and complementing the provisions of Law No 67/98 of 26 October (Law on Protection of Personal Data).

3 -...

4 -...

5 - In the situations provided for in the preceding paragraph, companies providing publicly available electronic communications services shall establish internal procedures for responding to requests for access to users’ personal data presented by the competent judicial authorities, in compliance with the referred special legislation.
Article 2
[...]
1 -...

a) «Communication» means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service;

b) «Electronic mail» means 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;

c) ...

d) ...

e) «Location data» 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;

f) ...

g) «Personal data breach» means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services.

2 - Point a) of the preceding paragraph shall not apply to information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the subscriber of an electronic communications service or any identifiable user receiving the information.

3 - Save for a specific definition established herein, the definitions in the Law on Protection of Personal Data and Law No 5/2004, of 10 February, as amended by Law No 51/2011, of 13 September (Electronic Communications Law) shall apply.

Article 3
Security of processing

1 - Providers of publicly available electronic communications services shall take appropriate technical and organisational measures to ensure the security of their services, where appropriate, as regards the network security, in conjunction with the provider of the public communications network.

2 - The provider of the public communications network supporting publicly available electronic communications services provided by a different company shall meet the requests presented by the latter, required to comply with the regime set out herein.

3 - Measures referred to in paragraph 1 shall be appropriate to the prevention of risks, having regard to the proportionality of implementation costs and the state of technological development.

4 - ICP - Autoridade Nacional das Comunicações (ICP-ANACOM) shall issue recommendations about best practices concerning the level of security which those measures should achieve.

5 - ICP-ANACOM shall audit the measures adopted under the preceding paragraphs, either directly or through an independent body.
6 - ICP-ANACOM shall lay down a plan for these audits, so as to specifically cover reference procedures and standards to be applied to them as well as requirements for auditors.

7 - ICP-ANACOM, or an independent body appointed by it, shall be entitled to carry out extraordinary security audits.

8 - For the purpose of paragraphs 4 to 7 of this article, where measures that involve matters of protection of personal data are concerned, ICP-ANACOM shall request the opinion of the Comissão Nacional de Protecção de Dados (CNPD - the National Data Protection Committee).

9 - Without prejudice to the Law on Protection of Personal Data, measures referred in paragraphs 1 to 3 shall include at least:

a) Measures that ensure that personal data can be accessed only by authorised personnel, and only for legally authorised purposes;

b) The protection of personal data transmitted, stored or otherwise processed, against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to;

c) Measures that ensure a security policy with respect to the processing of personal data.

10 - In case of a particular risk of a breach of the security of the network, providers of publicly available electronic communications services shall inform the subscribers free of charge concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

**Article 5**

[...]

1 - The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with the Law on Protection of Personal Data, inter alia, about the purposes of the processing.

2 - Nothing in this article and in the preceding article shall prevent any technical storage or access:

a) For the sole purpose of carrying out the transmission of a communication over an electronic communications network;

b) As strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

**Article 6**

[...]

1 - ....

2 -....

3 -....

4 - Providers of electronic communications services shall only process the data referred to in paragraph 1 where the subscriber or user to whom the data relate has given his or her prior and explicit consent, which may be withdrawn at any time, and to the extent and for the duration necessary for the purpose of marketing electronic communications services or for the provision of value added services.
Article 7

[...]

1 - [...]

2 - [...]

3 - Likewise, the processing of location data shall be allowed to the extent and for the duration necessary for the provision of value added services, insofar as prior and explicit consent has been obtained from subscribers or users.

4 - [...]

5 - [...]

6 - [...]

Article 8

[...]

1 - [...]

2 - Providers of publicly available electronic communications networks and/or services shall reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, namely by submitting proposals to CNPD regarding means which grant to subscribers an anonymous or strictly private access to publicly available electronic communications services.

3 - The approval by CNPD, referred to in the preceding paragraph, is subject to a compulsory opinion from ICP-ANACOM.

4 - [...]

Article 14

[...]

1 - The following irregularities shall be deemed as breaches liable to a fine from €1500 to €25 000, where committed by natural persons, and from €5000 to €5 000 000, where committed by legal persons:

a) Failure to observe network security standards imposed pursuant to paragraphs 1, 2, 3 and 10 of article 3;

b) Failure to observe standards of security in the processing of personal data imposed pursuant to paragraph 9 of article 3;

c) Violation of obligations laid down in paragraphs 1, 2, 3, 4, 5 and 10 of article 3-A or determined pursuant to the respective paragraphs 6 and 9;

d) Violation of the obligation established in paragraph 1 of article 4, of the prohibition established in paragraph 2 of article 4 and the carrying out of recordings in violation of paragraph 3 of article 4;
e) Failure to observe conditions of storage or access to information provided for in article 5;

f) The sending of communications for direct marketing purposes in violation of paragraphs 1 and 2 of article 13-A;

g) Violation of obligations imposed pursuant to paragraph 3 of article 13-A;

h) The sending of electronic mail in violation of paragraph 4 of article 13-A;

i) Violation of the obligation established pursuant to paragraph 1 of article 13-B;

j) Violation of paragraph 3 of article 13-B by bodies provided for in paragraph 1 thereof;

k) Violation of the obligation to provide information established pursuant to article 13-E;

l) Failure to comply with orders or determinations issued by CNPD pursuant to article 13-D and duly communicated to their addressees;

m) Failure to comply with orders or determinations issued by ICP-ANACOM pursuant to article 13-D and duly communicated to their addressees.

2 - The following irregularities shall be deemed as breaches liable to a fine from €500 to €20000, where committed by natural persons, and from €2500 to €2 500 000, where committed by legal persons:

a) Violation of notification requirements provided for in paragraphs 7, 8 and 10 of article 3-A or determined pursuant to paragraph 9;

b) Failure to observe conditions of processing and storage of traffic data and location data provided for in articles 6 and 7;

c) Violation of obligations established pursuant to paragraphs 1, 2 and 4 of article 8 and in article 9 to 11;

d) Violation of obligations established pursuant to article 10;

e) Violation of article 13.

3 - Whether the breach results from failure to comply with a legal duty or with an order or determination issued by the CNPD or ICP-ANACOM, in the respective fields of competence, penalties applied or compliance therewith shall not exempt the offender from fulfilling the duty or order, where possible.

4 - CNPD or ICP-ANACOM, in the respective fields of competence, are entitled to order the offender to fulfil the duty or order under consideration, on pain of a periodic penalty payment under the terms of article 15-C.

5 - Attempted breaches or breaches committed by negligence shall be punishable, minimum and maximum limits of fines being reduced by half.

Article 15

[...]

1- It is incumbent upon CNPD to initiate, examine and close breach proceedings as well as to apply admonitions, fines and additional penalties, for violation of paragraph 9 of article 3, article 3-A, paragraph 3 of article 4, articles 5, 6 and 7, paragraphs 1, 2 and 4 of article 8, article 10, article 13, paragraphs 1 to 4 of article 13-A, paragraphs 1 to 3 of article 13-B and paragraph 1 l) of article 14.
2 - It is incumbent upon ICP-ANACOM to initiate, examine and close breach proceedings as well as to apply admonitions, fines and additional penalties, for violation of paragraphs 1, 2, 3 and 10 of article 3, paragraphs 1 and 2 of article 4, article 9, article 11, article 13-E and paragraph 1 m) of article 14.

3 - The Management Board of ICP-ANACOM shall initiate breach proceedings and shall apply the penalties corresponding to the infringements provided for in the preceding paragraph, the examination thereof being incumbent upon the respective services.

4 - (Former paragraph 3).

5 - The amount of fines applied shall revert to the State at 60% and at 40% to CNPD or to ICP-ANACOM, as appropriate.»

Article 3
Addition to Law No 41/2004, of 18 August


«Article 3-A
Notification of a personal data breach

1 - Providers of publicly available electronic communications services shall, without undue delay, notify the personal data breach to CNPD.

2 - Where the personal data breach referred to in the preceding paragraph is likely to adversely affect the personal data of the subscriber or user, providers of publicly available electronic communications services shall also notify the subscriber or user of the breach, without undue delay, in order to allow them to take the necessary precautions.

3 - A personal data breach should be considered as adversely affecting the data or privacy of a subscriber or user where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision and use of publicly available communications services.

4 - The regime provided for in paragraph 2 shall not be required where providers of publicly available electronic communications services demonstrate to the satisfaction of CNPD that they implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach.

5 - Measures referred to in the preceding paragraph shall render the data unintelligible to any person who is not authorised to access it.

6 - Without prejudice to the provider’s notification obligation referred to in paragraph 2, if the provider has not already notified the subscriber or user of the personal data breach, CNPD may require it to do so, having considered the likely adverse effects of the breach.

7 - The minimum elements of the notification referred to in paragraph 2 shall be the identification of the nature of the personal data breach and the contact points where more information can be obtained, as well as the recommendation of measures to mitigate the possible adverse effects of the personal data breach.

8 - In the notification to CNPD provided for in paragraph 1, the provider of publicly available electronic communications services shall, in addition to elements mentioned in the preceding paragraph, describe the consequences of the personal data breach, and the measures proposed or taken by the provider to address it.
9 - In conformity with decisions of the European Commission, CNPD may issue guidelines and instructions concerning the circumstances in which providers of publicly available electronic communications services are required to notify personal data breaches, as well as the format of such notification and the manner in which the notification is to be made.

10 - Providers of publicly available electronic communications services shall establish and maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and measures adopted, including notifications made and the remedial action taken, in order to enable CNPD to verify compliance with obligations established in this article.

**Article 13-A**

**Unsolicited communications**

1 - The sending of unsolicited communications for direct marketing purposes, namely the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications, shall be subject to the prior and explicit consent of a subscriber who is a natural person, or of a user.

2 - The preceding paragraph shall not apply to subscribers who are legal persons, and unsolicited communication for direct marketing purposes shall be allowed until subscribers refuse future communications and enter themselves in the list provided for in paragraph 2 of article 13-B.

3 - The preceding paragraphs shall not prevent a provider of a given product or service, who obtained from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with the Law on Protection of Personal Data, from using such electronic contact details for direct marketing of its own similar products or services, provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details:

a) At the time of their collection; and

b) On the occasion of each message, in case the customer has not initially refused such use.

4 - The practice of sending electronic mail for the purpose of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, in violation of article 21 of Decree-Law No 7/2004, of 7 January, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that article, shall be prohibited.

5 - Providers of publicly available electronic communications services shall be entitled to bring legal proceedings against the offender of any of the provisions in this article, as well as in article 13-B, to protect the interests of their clients, as part of their own business interests.

**Article 13-B**

**Lists for the purpose of unsolicited communications**

1 - Bodies that promote the sending of communications for direct marketing purposes, namely through the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications, shall keep, on their own or through representative bodies, an up-to-date list of persons that gave clearly and free of charge their consent to receive this type of communications, as well as of clients who did not object to the reception thereof, under paragraph 3 of article 13-A.
2 - It shall be incumbent upon the Direção-Geral do Consumidor (DGC - the Consumer General Directorate) to keep an updated national list of legal persons who express their wish not to receive unsolicited communications for direct marketing purposes.

3 - No amount shall be charged for the entry in lists referred to in the preceding paragraphs.

4 - The entry in the list referred to in paragraph 2 depends on the completion of an electronic form available on the DGC website.

5 - Bodies that promote the sending of communications for direct marketing purposes shall consult the list, updated on a monthly basis by DGC, which shall make it available upon their request.

**Article 13-C**

**Cross-border cooperation**

1 - Without prejudice to competences assigned to other bodies, CNPD and ICP-ANACOM may adopt measures in the respective fields of competence to ensure effective cross-border cooperation in the enforcement of this law.

2 - Whenever CNPD and ICP-ANACOM wish to take action according to the preceding paragraph, the Authorities shall provide the European Commission, in good time before adopting any measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action.

**Article 13-D**

**Competences of CNPD and ICP-ANACOM**

In the scope of competences assigned under this law, CNPD and ICP-ANACOM are entitled, in the respective fields of competence, to:

   a) Draw up regulations on practises to be adopted to comply with this law;

   b) Give orders and make recommendations;

   c) Publish in the respective websites any codes of conduct they are aware of;

   d) Publish in the respective websites any other information deemed to be relevant.

**Article 13-E**

**Provision of information**

1 - Bodies subject to obligations under this law must provide, where requested, to ICP-ANACOM, in the respective field of competence, all information related to their activity, so that these authorities may exercise all powers provided for herein.

2 - The requests for information referred to in the preceding paragraph shall be appropriate to their intended aims, comply with the principle of proportionality and be duly substantiated.

3 - The requested information shall be submitted within the time limits, and in the form and to the level of detail required by ICP-ANACOM, which may establish the situations and periodicity governing the submission of such information.

4 - For the purposes of the paragraph 1, bodies shall identify, in a substantiated manner, any information deemed to be confidential, attaching, where appropriate, a non-confidential copy of documents comprising such information.
Article 13-F
Non-compliance

1 - Without prejudice to other applicable penalty mechanisms, where CNPD or ICP-ANACOM, in the respective fields of competence, find an infraction with any obligation arising under this law, they shall notify the offender of such findings, giving it the opportunity to state its views within a period of no less than 10 days, and, where appropriate, to cease the breach.

2 - After holding a hearing according to the preceding paragraph, CNPD or ICP-ANACOM, in the respective fields of competence, are entitled to require the offender to cease the breach immediately or within a reasonable time limit set for the purpose.

3 - Where the offender fails to cease the breach within the time-limit referred in the preceding paragraphs, CNPD or ICP-ANACOM, in the respective fields of competence, are entitled to take the adequate and proportional measures to guarantee compliance with obligations referred to in paragraph 1 hereof, namely the application of compulsory penalty payments as provided for by this law.

Article 13-G
Monitoring

It is incumbent on CNPD or ICP-ANACOM, in the respective fields of competence, established pursuant to article 15, to enforce the provisions of this law, through members and technical staff duly appointed by CNPD, pursuant to the Law on Protection of Personal Data, or monitoring agents or representatives duly qualified by ICP-ANACOM, pursuant to article 112 of the Electronic Communications Law.

Article 15-A
Additional penalties

1 - In the scope of breaches provided for in paragraph 2 of article 15, where justified by the seriousness of the offence and the degree of fault of the offender, ICP-ANACOM is entitled to apply the additional penalty of confiscation of objects, equipment and illicit devices, including any benefit obtained by the offender from the practise of the breach.

2 - Whoever fails to comply with an imposed additional penalty commits the crime of qualified disobedience.

Article 15-B
Confiscation

1 - Without prejudice to paragraph 1 of the preceding article, objects, equipment and illicit devices that have been seized provisionally by ICP-ANACOM, as a precautionary measure, and that, after notification for collection by interested parties, are not claimed within 60 days, shall be deemed to be confiscated.

2 - Confiscated objects, equipment or illicit devices shall revert to ICP-ANACOM, which shall dispose of them as deemed appropriate.

Article 15-C
Compulsory penalty payments

1 - Without prejudice to other applicable penalties, in case of failure to comply with decisions issued by CNPD or ICP-ANACOM imposing administrative penalties or, in the exercise of legally assigned powers, ordering the addressees of this law to adopt behaviours or measures, those authorities are entitled to impose a compulsory penalty payment, which must be duly substantiated, in the cases provided for in paragraphs 1, 3, 4 and 5 of article 10, paragraphs 1, 3, and 4 of article 13 and points a) to i), j) and l) to m) of paragraph 1 and a), b), c), d) and e) of paragraph 2 of article 14.
2 - The compulsory penalty payment shall consist of the imposition on the addressee of the payment of a pecuniary amount for each day of non-compliance beyond the deadline set for such compliance.

3 - The sanction referred to in the preceding paragraphs shall be determined according to criteria of reasonability and proportionality, having regard to the economic situation of the offender, namely its turnover in the preceding civil year, and with regard to the negative impact of the non-compliance on the market and on users, the daily amount of which sanction shall range from €500 to €100 000.

4 - The amounts established pursuant to the preceding paragraph may vary for each day of non-compliance, in an increasing trend, and shall not exceed the maximum amount of €3 000 000 or the maximum period of 30 days.

5 - The amount of the applied sanction shall revert to the State at 60% and to CNPD or ICP-ANACOM at 40%.

6 - Appeals may be lodged against acts of CNPD or ICP-ANACOM practiced under this article, according to whether such acts are practised in the scope of breach or administrative proceedings, under legislation that applies to each type of proceedings concerned.»

**Article 4**

**Amendment to Decree-Law No 7/2004, of 7 January**

Articles 7, 8, 9, 23, 36 and 37 of Decree-Law No 7/2004, of 7 January, as amended by Decree-Law No 62/2009, of 10 March, are hereby amended to read as follows:

«**Article 7**

**Restrictive measures**

1 - Measures restricting the free movement of an information society service from another Member State of the European Union may be adopted, including specific steps against a service provider, where such service causes or threatens to cause serious prejudice to:

   a) ... 
   b) ... 
   c) ... 
   d) ...

2 - The adoption shall be preceded by:

   a) ...

b) In case the Member State has not done so, or the measures taken are deemed to be inappropriate, a notification to the Commission and the Member State of origin of the intention to take the restrictive measures.

3 - ...

4 - The measures adopted shall be proportionate to the interests to be safeguarded.

**Article 8**

[...]

...
In the case of urgency, the competent entities, including courts, are entitled to take restrictive measures, not preceded by notifications to the Commission and to the other Member States of origin, provided for in the preceding article.

**Article 9**

[...]

1 - [...]

2 - The competent entities that wish to take restrictive measures, or actually take them, shall immediately communicate this fact to the central supervisory authority, so that such measures are promptly notified to the Commission and to the Member States of origin.

3 - As regards urgent restrictive measures, grounds of urgency in the adoption of the measures shall also be indicated.

**Article 23**

[...]

1 - Electronic remote advertising communications in the scope of regulated professions shall be allowed insofar as rules on professional ethics of each profession are complied with, as regards independence, professional secrecy and loyalty towards the public and among members of the profession.

2 - [...]

**Article 36**

[...]

1 - [...]

2 - [...]

a) Adopt the restrictive measures provided for in articles 7 and 8;

b) [...]

c) [...]

d) [...]

e) [...]

3 - [...]

4 - [...]

**Article 37**

[...]

1 - [...]

a) Failure to make available or to provide to addressees the information provided for in articles 10, 13 and 21, and in paragraph 1 of article 28;

b) *(Repealed).*
c) ...

d) ...

e) ...

f) ...

2 -...

3 -...

4 -...

5 -...»

Article 5
Repealing provision

The following statutory instruments are hereby repealed:

a) Article 12 of Law No 41/2004, of 18 August;

b) Article 22 and point b) of paragraph 1 of article 37 of Decree-Law No 7/2004, of 7 January, as amended by Decree-Law No 62/2009, of 10 March.

Article 6
Republication

Law number 41/2004, of 18 August, with the current wording, is republished in annex to this statutory instrument, of which it is an integral part.

Article 7
Entry into force

This statutory instrument shall enter into force of the day following that of its publication.

Approved on 25 July 2012.

The President of the Assembly of the Republic, Maria da Assunção A. Esteves.

Promulgated on 10 August 2012.

Let it be published.

The President of the Republic, ANÍBAL CAVACO SILVA.

Countersigned on 17 August, 2012.

The Prime Minister, Pedro Passos Coelho.

ANNEX

(referred to in article 6)
Republication of Law number 41/2004, of 18 August

CHAPTER I
Subject-matter and scope

Article 1
Subject-matter and scope of application


2 - This law shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks, including public communications networks supporting data collection and identification devices, specifying and complementing the provisions of Law No 67/98 of 26 October (Law on Protection of Personal Data).

3 - The provisions of the present law shall ensure protection of the legitimate interests of subscribers who are legal persons, to the extent that such protection is consistent with their nature.

4 - The exceptions to the application of the present law that are strictly necessary for the protection of activities concerning public security, defence, State security, and the prevention, investigation and prosecution of criminal offences shall be defined in special legislation.

5 - In the situations provided for in the preceding paragraph, companies providing publicly available electronic communications services shall establish internal procedures for responding to requests for access to users’ personal data presented by the competent judicial authorities, in compliance with the referred special legislation.

Article 2
Definitions

1 - For the purposes of the present law, the following definitions shall apply:

a) «Communication» means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service;

b) «Electronic mail» means 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;

c) «User» means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service;

d) «Traffic data» means any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof;

e) «Location data» 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;
f) «Value added service» means any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof;

g) «Personal data breach» means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services.

2 - Point a) of the preceding paragraph shall not apply to information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the subscriber of an electronic communications service or any identifiable user receiving the information.

3 - Save for a specific definition established herein, the definitions in the Law on Protection of Personal Data and Law No 5/2004, of 10 February, as amended by Law No 51/2011, of 13 September (Electronic Communications Law) shall apply.

CHAPTER II
Security and confidentiality

Article 3
Security of processing

1 - Providers of publicly available electronic communications services shall take appropriate technical and organisational measures to ensure the security of their services, where appropriate, as regards the network security, in conjunction with the provider of the public communications network.

2 - The provider of the public communications network supporting publicly available electronic communications services provided by a different company shall meet the requests presented by the latter, required to comply with the regime set out herein.

3 - Measures referred to in paragraph 1 shall be appropriate to the prevention of risks, having regard to the proportionality of implementation costs and the state of technological development.

4 - ICP - Autoridade Nacional das Comunicações (ICP-ANACOM) shall issue recommendations about best practices concerning the level of security which those measures should achieve.

5 - ICP-ANACOM shall audit the measures adopted under the preceding paragraphs, either directly or through an independent body.

6 - ICP-ANACOM shall lay down a plan for these audits, so as to specifically cover reference procedures and standards to be applied to them as well as requirements for auditors.

7 - ICP-ANACOM, or an independent body appointed by it, shall be entitled to carry out extraordinary security audits.

8 - For the purpose of paragraphs 4 to 7 of this article, where measures that involve matters of protection of personal data are concerned, ICP-ANACOM shall request the opinion of the Comissão Nacional de Protecção de Dados (CNPD - the National Data Protection Committee).

9 - Without prejudice to the Law on Protection of Personal Data, measures referred in paragraphs 1 to 3 shall include at least:

a) Measures that ensure that personal data can be accessed only by authorised personnel, and only for legally authorised purposes;
b) The protection of personal data transmitted, stored or otherwise processed, against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to;

c) Measures that ensure a security policy with respect to the processing of personal data.

10 - In case of a particular risk of a breach of the security of the network, providers of publicly available electronic communications services shall inform the subscribers free of charge concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

Article 3-A
Notification of a personal data breach

1 - Providers of publicly available electronic communications services shall, without undue delay, notify the personal data breach to CNPD.

2 - Where the personal data breach referred to in the preceding paragraph is likely to adversely affect the personal data of the subscriber or user, providers of publicly available electronic communications services shall also notify the subscriber or user of the breach, without undue delay, in order to allow them to take the necessary precautions.

3 - A personal data breach should be considered as adversely affecting the data or privacy of a subscriber or user where it could result in, for example, identity theft or fraud, physical harm, significant humiliation or damage to reputation in connection with the provision and use of publicly available communications services.

4 - The regime provided for in paragraph 2 shall not be required where providers of publicly available electronic communications services demonstrate to the satisfaction of CNPD that they implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach.

5 - Measures referred to in the preceding paragraph shall render the data unintelligible to any person who is not authorised to access it.

6 - Without prejudice to the provider’s notification obligation referred to in paragraph 2, if the provider has not already notified the subscriber or user of the personal data breach, CNPD may require it to do so, having considered the likely adverse effects of the breach.

7 - The minimum elements of the notification referred to in paragraph 2 shall be the identification of the nature of the personal data breach and the contact points where more information can be obtained, as well as the recommendation of measures to mitigate the possible adverse effects of the personal data breach.

8 - In the notification to CNPD provided for in paragraph 1, the provider of publicly available electronic communications services shall, in addition to elements mentioned in the preceding paragraph, describe the consequences of the personal data breach, and the measures proposed or taken by the provider to address it.

9 - In conformity with decisions of the European Commission, CNPD may issue guidelines and instructions concerning the circumstances in which providers of publicly available electronic communications services are required to notify personal data breaches, as well as the format of such notification and the manner in which the notification is to be made.

10 - Providers of publicly available electronic communications services shall establish and maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and measures adopted, including notifications made and the remedial action taken, in order to enable CNPD to verify compliance with obligations established in this article.
Article 4
Inviolability of electronic communications

1 - Undertakings providing electronic communications networks and/or services shall ensure the inviolability of communications and the related traffic data by means of a public communications networks and publicly available electronic communications services.

2 - Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users is prohibited, without the prior and explicit consent of the users concerned, except for cases provided for in the law.

3 - The provision in the present article shall not affect any legally authorised recording of communications and the related traffic data, when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction, nor of any other communication made in the scope of a business relationship, provided that the data holder has been informed thereof and given his consent thereto.

4 - Recordings of communications by and for public services intended to provide for emergency situations of any nature shall be authorized.

Article 5
Storage and access to information

1 - The storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user shall only be allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with the Law on Protection of Personal Data, inter alia, about the purposes of the processing.

2 - Nothing in this article and in the preceding article shall prevent any technical storage or access:

   a) For the sole purpose of carrying out the transmission of a communication over an electronic communications network;

   b) As strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

Article 6
Traffic data

1 - Without prejudice to the following articles, traffic data relating to subscribers and users which have been processed and stored by undertakings providing electronic communications networks and/or services shall be erased or made anonymous where they are no longer needed for the purpose of the transmission of a communication.

2 - The processing of traffic data necessary for the purposes of subscriber billing and interconnection payments shall be permitted, namely:

   a) Number or identification, address and type of station of the subscriber;

   b) Total number of units to be charged for the accounting period, as well as the type, starting time and duration of the calls made and/or the data volume transmitted;

   c) Date of the call or service and called number;
d) Other information concerning payments such as advance payment, payments by instalments, disconnection and reminders.

3 - The processing referred to in the preceding paragraph shall be permissible only up to the end of the period during which the bill may lawfully be challenged or the payment be pursued.

4 - Providers of electronic communications services shall only process the data referred to in paragraph 1 where the subscriber or user to whom the data relate has given his or her prior and explicit consent, which may be withdrawn at any time, and to the extent and for the duration necessary for the purpose of marketing electronic communications services or for the provision of value added services.

5 - For the purposes mentioned in paragraph 2 and, prior to obtaining consent from subscribers or users, for the purposes mentioned in paragraph 4, undertakings providing electronic communications services shall provide them accurate and full information on the types of traffic data which are processed, the purposes and the duration of such processing, as well as on a possible transmission to a third party for the purpose of providing the value added service.

6 - The processing of traffic data shall be restricted to workers and employees of undertakings providing electronic communications networks and/or publicly available services who are responsible for handling billing or traffic management, customer enquiries, fraud detection, marketing publicly available electronic communications services or providing a value added service, and shall be restricted to what is necessary for the purposes of such activities.

7 - The preceding paragraphs shall apply without prejudice to the possibility for courts or other competent bodies to be informed of traffic data, in conformity with applicable legislation with a view to settling disputes, in particular interconnection or billing disputes.

**Article 7**

**Location data**

1 - Where location data other than traffic data, relating to subscribers or users of public communications networks or publicly available electronic communications services, are processed, such data may only be processed when they are made anonymous.

2 - The record, processing and transmission of location data to bodies with legal competence to deal with emergency calls, for the purpose of responding to such calls, shall be permitted.

3 - Likewise, the processing of location data shall be allowed to the extent and for the duration necessary for the provision of value added services, insofar as prior and explicit consent has been obtained from subscribers or users.

4 - Undertakings providing publicly available electronic communications services shall, namely, inform the users or subscribers, prior to obtaining their consent, of the type of location data which will be processed, of the duration and purposes of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service.

5 - Undertakings providing publicly available electronic communications services shall guarantee subscribers and users the possibility, using a simple means and free of charge:

a) To withdraw at any time their consent previously given for the processing of location data referred to in the preceding paragraphs;

b) To temporarily refuse the processing of such data for each connection to the network or for each transmission of a communication.
6 - Processing of location data shall be restricted to workers and employees of undertakings providing electronic communications networks and/or publicly available services or of the third party providing the value added service, and shall be restricted to what is necessary for the purposes of the referred activity.

**Article 8**

**Itemised billing**

1 - Subscribers shall have the right to receive non-itemised bills.

2 - Providers of publicly available electronic communications networks and/or services shall reconcile the rights of subscribers receiving itemised bills with the right to privacy of calling users and called subscribers, namely by submitting proposals to CNPD regarding means which grant to subscribers an anonymous or strictly private access to publicly available electronic communications services.

3 - The approval by CNPD, referred to in the preceding paragraph, is subject to a compulsory opinion from ICP-ANACOM.

4 - Calls that are free of charge to the calling subscriber, including calls to emergency services or helplines, shall not be identified in the calling subscriber's itemised bill.

**Article 9**

**Identification of calling line and connected line**

1 - Where presentation of calling line identification is offered, undertakings providing publicly available electronic communications services shall offer the calling subscribers, on a per-line basis, and the calling remaining users on a per-call basis, the possibility, using a simple means and free of charge, of preventing the presentation of the calling line identification.

2 - Where presentation of calling line identification is offered, undertakings providing publicly available electronic communications services shall offer the called subscriber the possibility, using a simple means and free of charge for reasonable use of this function, of preventing the presentation of the calling line identification of incoming calls.

3 - Where presentation of calling line identification is offered prior to the call being established, undertakings providing publicly available electronic communications services shall offer the called subscriber the possibility, using a simple means, of rejecting non-identified incoming calls.

4 - Where presentation of connected line identification is offered, undertakings providing publicly available electronic communications services shall 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 - The provision of paragraph 1 of the present article shall also apply with regard to calls to countries outside the European Union originating in national territory.

6 - The provisions of paragraphs 2, 3 and 4 shall also apply to incoming calls originating in countries outside the European Union.

7 - Undertakings providing electronic communications networks and/or publicly available services shall provide the public, especially subscribers, with transparent and up-to-date information on the possibilities referred to in the preceding paragraphs.

**Article 10**

**Exceptions**
1 - Undertakings providing electronic communications networks and/or publicly available services, where compatible with the principles of necessity, appropriateness and proportionality, shall cancel, for a period of time not exceeding 30 days, the elimination of the presentation of the calling line identification, on a written and duly substantiated request from a subscriber who wishes to determine the origin of non-identified calls that upset the peace of the family or the intimacy of private life, in which case the telephone number of calling subscribers who have prevented the line identification shall be recorded and made available to the called subscriber.

2 - In the cases provided for in the preceding paragraph, the cancellation of the elimination of the presentation of the calling line shall be preceded of a compulsory opinion on the part of CNPD.

3 - Undertakings referred to in paragraph 1 shall also cancel, on a per-line basis, the elimination of the presentation of calling line as well as record and make available the location data of a subscriber or user, in the case provided for in paragraph 2 of article 7, in order to make available such data to bodies with legal competence to receive emergency calls for the purpose of responding to such calls.

4 - In the cases provided for in the preceding paragraphs, prior information shall be compulsorily transmitted to the holder of the referred data, on the transmission thereof, to the subscriber who required them pursuant to paragraph 1 or to the emergency services pursuant to paragraph 3.

5 - The information duty regarding data holders shall be performed through the following means:

a) In the cases mentioned in paragraph 1, through the broadcast of an automatic recording before the call is established, that informs the data holder that, from that moment and for the set period of time, his telephone number ceases to be confidential concerning calls to the subscriber who requested the number identification;

b) In the cases mentioned in paragraph 3, through the inclusion of general contractual terms in contracts signed between subscribers and undertakings providing electronic communications networks and/or services, or through explicit notification given to subscribers of contracts already signed, which allow the transmission of that information to emergency services.

6 - The record and notification referred to in paragraphs 1 and 3 shall be disclosed to the public and the use thereof shall be restricted to the intended purposes.

**Article 11**

**Automatic call forwarding**

Undertakings providing electronic communications networks and/or publicly available services shall ensure that any subscriber has the possibility, using a simple means and free of charge, of stopping automatic call forwarding by a third party to the subscriber’s terminal equipment.

**Article 12**

*(Repealed.)*

**Article 13**

**Directories of subscribers**

1 - Subscribers shall be informed, free of charge and before the respective data are included in printed or electronic directories, available to the public or obtainable through directory enquiry services, about:
a) The intended purposes of such directories;

b) Any further usage possibilities based on search functions embedded in electronic versions of the directories.

2 - Subscribers shall be given the opportunity to determine whether their personal data are included in a public directory, and if so, which, to the extent that such data are relevant for the purposes of the directories, as determined by the provider of the directories.

3 - Subscribers shall be given the opportunity to verify, correct, alter or withdraw the data included in the referred directories, free of charge.

4 - Additional consent shall be asked of the subscribers for any purpose of a public directory other than the search of contact details of persons on the basis of their name and, where necessary, a minimum of other elements of identification.

**Article 13-A**

Unsolicited communications

1 - The sending of unsolicited communications for direct marketing purposes, namely the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines or electronic mail, including SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications, shall be subject to the prior and explicit consent of a subscriber who is a natural person, or of a user.

2 - The preceding paragraph shall not apply to subscribers who are legal persons, and unsolicited communication for direct marketing purposes shall be allowed until subscribers refuse future communications and enter themselves in the list provided for in paragraph 2 of article 13-B.

3 - The preceding paragraphs shall not prevent a provider of a given product or service, who obtained from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, in accordance with the Law on Protection of Personal Data, from using such electronic contact details for direct marketing of its own similar products or services, provided that customers clearly and distinctly are given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details:

a) At the time of their collection; and

b) On the occasion of each message, in case the customer has not initially refused such use.

4 - The practice of sending electronic mail for the purpose of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, in violation of article 21 of Decree-Law No 7/2004, of 7 January, which do not have a valid address to which the recipient may send a request that such communications cease or which encourage recipients to visit websites that contravene that article, shall be prohibited.

5 - Providers of publicly available electronic communications services shall be entitled to bring legal proceedings against the offender of any of the provisions in this article, as well as in article 13-B, to protect the interests of their clients, as part of their own business interests.

**Article 13-B**

Lists for the purpose of unsolicited communications

1 - Bodies that promote the sending of communications for direct marketing purposes, namely through the use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines or electronic mail, including
SMS (Short Message Service), EMS (Enhanced Message Service) and MMS (Multimedia Message Service) and other kinds of similar applications, shall keep, on their own or through representative bodies, an up-to-date list of persons that gave clearly and free of charge their consent to receive this type of communications, as well as of clients who did not object to the reception thereof, under paragraph 3 of article 13-A.

2 - It shall be incumbent upon the Direção-Geral do Consumidor (DGC - the Consumer General Directorate) to keep an updated national list of legal persons who express their wish not to receive unsolicited communications for direct marketing purposes.

3 - No amount shall be charged for the entry in lists referred to in the preceding paragraphs.

4 - The entry in the list referred to in paragraph 2 depends on the completion of an electronic form available on the DGC website.

5 - Bodies that promote the sending of communications for direct marketing purposes shall consult the list, updated on a monthly basis by DGC, which shall make it available upon their request.

Article 13-C
Cross-border cooperation

1 - Without prejudice to competences assigned to other bodies, CNPD and ICP-ANACOM may adopt measures in the respective fields of competence to ensure effective cross-border cooperation in the enforcement of this law.

2 - Whenever CNPD and ICP-ANACOM wish to take action according to the preceding paragraph, the Authorities shall provide the European Commission, in good time before adopting any measures, with a summary of the grounds for action, the envisaged measures and the proposed course of action.

Article 13-D
Competences of CNPD and ICP-ANACOM

In the scope of competences assigned under this law, CNPD and ICP-ANACOM are entitled, in the respective fields of competence, to:

a) Draw up regulations on practises to be adopted to comply with this law;

b) Give orders and make recommendations;

c) Publish in the respective websites any codes of conduct they are aware of;

d) Publish in the respective websites any other information deemed to be relevant.

Article 13-E
Provision of information

1 - Bodies subject to obligations under this law must provide, where requested, to ICP-ANACOM, in the respective field of competence, all information related to their activity, so that these authorities may exercise all powers provided for herein.

2 - The requests for information referred to in the preceding paragraph shall be appropriate to their intended aims, comply with the principle of proportionality and be duly substantiated.
3 - The requested information shall be submitted within the time limits, and in the form and to the level of detail required by ICP-ANACOM, which may establish the situations and periodicity governing the submission of such information.

4 - For the purposes of the paragraph 1, bodies shall identify, in a substantiated manner, any information deemed to be confidential, attaching, where appropriate, a non-confidential copy of documents comprising such information.

CHAPTER III
Sanctioning regime

Article 13-F
Non-compliance

1 - Without prejudice to other applicable penalty mechanisms, where CNPD or ICP-ANACOM, in the respective fields of competence, find an infraction with any obligation arising under this law, they shall notify the offender of such findings, giving it the opportunity to state its views within a period of no less than 10 days, and, where appropriate, to cease the breach.

2 - After holding a hearing according to the preceding paragraph, CNPD or ICP-ANACOM, in the respective fields of competence, are entitled to require the offender to cease the breach immediately or within a reasonable time limit set for the purpose.

3 - Where the offender fails to cease the breach within the time-limit referred in the preceding paragraphs, CNPD or ICP-ANACOM, in the respective fields of competence, are entitled to take the adequate and proportional measures to guarantee compliance with obligations referred to in paragraph 1 hereof, namely the application of compulsory penalty payments as provided for by this law.

Article 13-G
Monitoring

It is incumbent on CNPD or ICP-ANACOM, in the respective fields of competence, established pursuant to article 15, to enforce the provisions of this law, through members and technical staff duly appointed by CNPD, pursuant to the Law on Protection of Personal Data, or monitoring agents or representatives duly qualified by ICP-ANACOM, pursuant to article 112 of the Electronic Communications Law.

Article 14
Breaches

1 - The following irregularities shall be deemed as breaches liable to a fine from €1500 to €25 000, where committed by natural persons, and from €5000 to €5 000 000, where committed by legal persons:

a) Failure to observe network security standards imposed pursuant to paragraphs 1, 2, 3 and 10 of article 3;

b) Failure to observe standards of security in the processing of personal data imposed pursuant to paragraph 9 of article 3;

c) Violation of obligations laid down in paragraphs 1, 2, 3, 4, 5 and 10 of article 3-A or determined pursuant to the respective paragraphs 6 and 9;

d) Violation of the obligation established in paragraph 1 of article 4, of the prohibition established in paragraph 2 of article 4 and the carrying out of recordings in violation of paragraph 3 of article 4;

e) Failure to observe conditions of storage or access to information provided for in article 5;
f) The sending of communications for direct marketing purposes in violation of paragraphs 1 and 2 of article 13-A;

g) Violation of obligations imposed pursuant to paragraph 3 of article 13-A;

h) The sending of electronic mail in violation of paragraph 4 of article 13-A;

i) Violation of the obligation established pursuant to paragraph 1 of article 13-B;

j) Violation of paragraph 3 of article 13-B by bodies provided for in paragraph 1 thereof;

k) Violation of the obligation to provide information established pursuant to article 13-E;

l) Failure to comply with orders or determinations issued by CNPD pursuant to article 13-D and duly communicated to their addressees;

m) Failure to comply with orders or determinations issued by ICP-ANACOM pursuant to article 13-D and duly communicated to their addressees.

2 - The following irregularities shall be deemed as breaches liable to a fine from €500 to €20 000, where committed by natural persons, and from €2500 to €2 500 000, where committed by legal persons:

a) Violation of notification requirements provided for in paragraphs 7, 8 and 10 of article 3-A or determined pursuant to paragraph 9;

b) Failure to observe conditions of processing and storage of traffic data and location data provided for in articles 6 and 7;

c) Violation of obligations established pursuant to paragraphs 1, 2 and 4 of article 8 and in article 9 to 11;

d) Violation of obligations established pursuant to article 10;

e) Violation of article 13.

3 - Whether the breach results from failure to comply with a legal duty or with an order or determination issued by the CNPD or ICP-ANACOM, in the respective fields of competence, penalties applied or compliance therewith shall not exempt the offender from fulfilling the duty or order, where possible.

4 - CNPD or ICP-ANACOM, in the respective fields of competence, are entitled to order the offender to fulfil the duty or order under consideration, on pain of a periodic penalty payment under the terms of article 15-C.

5 - Attempted breaches or breaches committed by negligence shall be punishable, minimum and maximum limits of fines being reduced by half.

Article 15

Procedure and application of fines

1- It is incumbent upon CNPD to initiate, examine and close breach proceedings as well as to apply admonitions, fines and additional penalties, for violation of paragraph 9 of article 3, article 3-A, paragraph 3 of article 4, articles 5, 6 and 7, paragraphs 1, 2 and 4 of article 8, article 10, article 13, paragraphs 1 to 4 of article 13-A, paragraphs 1 to 3 of article 13-B and paragraph 1 l) of article 14.
2 - It is incumbent upon ICP-ANACOM to initiate, examine and close breach proceedings as well as to apply admonitions, fines and additional penalties, for violation of paragraphs 1, 2, 3 and 10 of article 3, paragraphs 1 and 2 of article 4, article 9, article 11, article 13-E and paragraph 1 m) of article 14.

3 - The Management Board of ICP-ANACOM shall initiate breach proceedings and shall apply the penalties corresponding to the infringements provided for in the preceding paragraph, the examination thereof being incumbent upon the respective services.

4 - The competences provided for in the preceding article may be delegated.

5 - The amount of fines applied shall revert to the State at 60% and at 40% to CNPD or to ICP-ANACOM, as appropriate.

**Article 15-A**

**Additional penalties**

1 - In the scope of breaches provided for in paragraph 2 of article 15, where justified by the seriousness of the offence and the degree of fault of the offender, ICP-ANACOM is entitled to apply the additional penalty of confiscation of objects, equipment and illicit devices, including any benefit obtained by the offender from the practise of the breach.

2 - Whoever fails to comply with an imposed additional penalty commits the crime of qualified disobedience.

**Article 15-B**

**Confiscation**

1 - Without prejudice to paragraph 1 of the preceding article, objects, equipment and illicit devices that have been seized provisionally by ICP-ANACOM, as a precautionary measure, and that, after notification for collection by interested parties, are not claimed within 60 days, shall be deemed to be confiscated.

2 - Confiscated objects, equipment or illicit devices shall revert to ICP-ANACOM, which shall dispose of them as deemed appropriate.

**Article 15-C**

**Compulsory penalty payments**

1 - Without prejudice to other applicable penalties, in case of failure to comply with decisions issued by CNPD or ICP-ANACOM imposing administrative penalties or, in the exercise of legally assigned powers, ordering the addressees of this law to adopt behaviours or measures, those authorities are entitled to impose a compulsory penalty payment, which must be duly substantiated, in the cases provided for in paragraphs 1, 3, 4 and 5 of article 10, paragraphs 1, 3, and 4 of article 13 and points a) to i), j) and l) to m) of paragraph 1 and a), b), c), d) and e) of paragraph 2 of article 14.

2 - The compulsory penalty payment shall consist of the imposition on the addressee of the payment of a pecuniary amount for each day of non-compliance beyond the deadline set for such compliance.

3 - The sanction referred to in the preceding paragraphs shall be determined according to criteria of reasonability and proportionality, having regard to the economic situation of the offender, namely its turnover in the preceding civil year, and with regard to the negative impact of the non-compliance on the market and on users, the daily amount of which sanction shall range from €500 to €100 000.
4 - The amounts established pursuant to the preceding paragraph may vary for each day of non-compliance, in an increasing trend, and shall not exceed the maximum amount of €3 000 000 or the maximum period of 30 days.

5 - The amount of the applied sanction shall revert to the State at 60% and to CNPD or ICP-ANACOM at 40%.

6 - Appeals may be lodged against acts of CNPD or ICP-ANACOM practiced under this article, according to whether such acts are practised in the scope of breach or administrative proceedings, under legislation that applies to each type of proceedings concerned.

**Article 16**

**Subsidiary legislation**

The sanctioning rules comprised in articles 33 to 39 of the Law on Protection of Personal Data shall apply in all matters not provided for in the present law.

**CHAPTER IV**

**Final and transitory provisions**

**Article 17**

**Technical features and standardization**

1 - The compliance with the provisions of this law shall not determine that mandatory requirements for specific technical features are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment within the countries of the European Union.

2 - From the preceding paragraph are excepted the elaboration and issue of specific technical features necessary to the implementation of the present law, which shall be notified to the European Commission in accordance with the procedures provided for in Decree-Law no. 58/2000, of 18 April.

**Article 18**

**Transitory provisions**

1 - The provision of article 13 shall not apply to editions of directories already produced or placed on the market in printed or off-line electronic form before the present law enters into force.

2 - Where the personal data of subscribers to publicly available fixed or mobile voice telephony services have been included in a public subscriber directory, in conformity with prior legislation and before the entry into force of the present law, the personal data of such subscribers may remain included in that public directory in its printed or electronic versions.

3 - In the case provided for in the preceding paragraph, subscribers shall have the right to withdraw their personal data from the public directory in consideration, after having received complete information about purposes and options thereof, in accordance with article 13.

4 - The information referred to in the preceding paragraph shall be conveyed to subscribers within at the most six months from the date of entry into force of the present law.

**Article 19**

**Repeal**

Law no. 69/98, of 28 October, is hereby repealed.
Article 20
Entry into force

The present law shall enter into force on the day following that of its publication.