Coordinated text of the Act of 30 May 2005

- **laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector and**
- **amending Articles 88-2 and 88-4 of the Code of Criminal Procedure**

(Mém. A – 73 from 7 June 2005, p. 1168, doc. Parl. 5181; Dir. 2002/58/CE)

amended by

the Act of 2 August 2002,

the Act of 24 July 2010,

the Act of 28 July 2011.

Coordinated text from 10 August 2011

Version applicable from 1 September 2011

Art. 1. Scope

Without prejudice and subject to the general provisions concerning the protection of persons with regard to the processing of personal data or governing electronic communications networks and services, the following provisions apply specifically to the processing of such personal data in the context of the supply of publicly available electronic communications services over the public communications networks, *(Act of 28 July 2011)*" including public communications networks supporting data collection and identification devices."

Art. 2. Definitions

For the purposes of this Act:

(a) "subscriber" means a natural or legal person who or which is party to a contract with a provider offering publicly available electronic communication services for the supply of such services;
(b) "consent" means any freely given specific and informed indication of the data subject's wishes by which he or his legal, judicial or statutory representative signifies his agreement to personal data relating to him being processed;
(c) "communication" means any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service. This does not include any information conveyed as part of a broadcasting service to the public over an electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;
(d) "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;
(e) "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;
(f) "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;
(g) "Institute" means Institut Luxembourgeois de Régulation (Luxembourg Regulation Institute);
(h) "electronic communications network" means transmission systems and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio

and television broadcasting, and cable television networks, irrespective of the type of information conveyed;

(i) "public communications network" means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services. The provider of a public communications network is hereinafter referred to as the "operator";

(j) "electronic communications service" means a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. The supplier of electronic communications services is hereinafter referred to as the "service provider";

(k) "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;

(l) "user" means a natural or legal person using or requesting a publicly available electronic communications service for private or business purposes, without necessarily having subscribed to that service.
(Act of 28 July 2011)

(m) ""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 a publicly available electronic communications service.";

Art. 3. Security of processing

(1) The service provider must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the operator with respect to network security. In the event of any breach or serious risk of a breach of the security of the network or services, the service provider and, where necessary, the operator shall take appropriate remedial measures, at its/their sole expense.
(Act of 28 July 2011)
"Without prejudice to the amended Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data, the measures referred to in paragraph (1) shall at least:
- ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,
- protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,
- ensure the implementation of a security policy with respect to the processing of personal data,

The National Commission for Data Protection shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve."

(2) Without prejudice to the foregoing, the service provider and, where necessary, the operator must inform the subscribers of any imminent risk of a breach of the security of the network or services which may compromise the confidentiality of communications, and of any possible remedies, including an indication of the likely costs involved.
(Act of 28 July 2011)

(3) In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the National Commission for Data Protection.
When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.
Notification of a personal data breach to a subscriber or individual concerned

shall not be required if the provider has demonstrated to the satisfaction of the National Commission for Data Protection that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the National Commission for Data Protection, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the National Commission for Data Protection shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

The National Commission for Data Protection may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made.

In the case of a failure to comply with their notification obligations, providers are warned by the National Commission for Data Protection. In the case of repeted failure, the National Commission can impose a fine that cannot exceed 50.000 euros.

An appeal with the administrative court against the decisions taken by the National Commission is opened int the context of the present article.

(4) Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the National Commission for Data Protection to verify compliance with the provisions of paragraph (3). The inventory shall only include the information necessary for this purpose.

(5) Any person who contravenes the provisions of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.

Art. 4. Confidentiality of communications

(1) Each service provider or operator shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services.

(2) It is prohibited for persons other than users to listen, tap, store or to use other kinds of interception or surveillance of communications and the related traffic data, without the consent of the users concerned.

(3) Paragraph (2):

(a) shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality;
(Act of 28 July 2011)

(b) “shall not apply to authorities acting in the context of Article 67-1 of the Code of Criminal Procedure, or to authorities competent pursuant to Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard State security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences;”

(c) shall not apply to communications, or the traffic data relating thereto, made to the single European emergency number 112 or the emergency numbers determined by the Institute solely for the purposes of (a) enabling messages to be listened to again in the event of problems of comprehension or ambiguity as between the caller and the person called, (b) permitting the documentation of false alarms, threats and improper calls and (c) the production of evidence where there is any dispute as to the course or

conduct of action taken by way of assistance. Traffic data relating to the communications referred to above, including location data, shall be erased once the assistance has been provided. The content of such communications is to be erased on the expiry of a maximum period of six months;

(d) shall not affect the recording of communications and of the traffic data relating thereto where such recording is carried out in the context of lawful business practices *(Amended Act of 2 August 2002)* "for the purpose of providing evidence of a commercial transaction.
Parties to such transactions" shall be informed in advance of the fact that such recordings may be made, of the reason or reasons for which communications are recorded and of the maximum period for which the recordings may be retained. Recorded communications are to be erased as soon as the object is achieved and at all events upon the expiry of the legally prescribed period for contesting the transaction;
(Act of 28 July 2011)

(e) "shall not apply where electronic communications networks are used to store information or to gain access to information stored in the terminal equipment of a subscriber or user on condition that the subscriber or user concerned is provided with clear and comprehensive information, in particular about the purposes of the processing. The methods of providing information and offering the right to refuse should be as user-friendly as possible. Where it is technically possible and effective, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application.
This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."

(4) Any person who contravenes the provisions of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.

Art. 5. Traffic data

(1)

(a) "For the purposes of the investigation, detection and prosecution of criminal offences, subject to a criminal or correctional penalty of detention of up to one year, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing traffic data must retain such data for a period of 6 months from the date of the communication. The obligation to retain data shall include the retention of the data relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data) in the process of supplying the communication services concerned. The categories of traffic data capable of being used for the investigation, detection and prosecution of criminal offences shall be determined by Grand-Ducal Regulation."

(b) Upon the expiry of the retention period provided for in (a) above, the service provider or operator shall be required to erase or render anonymous traffic data relating to subscribers and users.

(2) Service providers or operators processing traffic data concerning subscribers or users shall be required to take all necessary steps to ensure the retention of such data for the period provided for in paragraph (1)(a) above, in such a way as to make it impossible for anyone to access the data in question once they are no longer needed for the transmission of a communication or for processing pursuant to paragraphs (3) and (4), with the exception of access which is:
(Act of 24 July 2010)

- "ordered by authorities acting in the context of Article 67-1 of the Code of Criminal Procedure, or by authorities competent pursuant to Articles 88-1 to

88-4 of the Code of Criminal Procedure to safeguard State security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences; or"
- requested by the competent bodies with a view to settling disputes, in particular interconnection or billing disputes.

(3) Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing shall be permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued, and may not in any event exceed a period of 6 months where the invoice has been paid and has not been disputed or challenged.

(4) Traffic data may be processed for the purposes of marketing electronic communications services or providing value added services, to the extent and for the duration necessary for such supply or marketing of such services, provided that the provider of an electronic communications service or the operator has informed the subscriber or user concerned in advance of the types of traffic data processed and of the purpose and duration of the processing, and provided that the subscriber or user has given his/her consent, notwithstanding his/her right to object to such processing at any time.

(5) Processing of traffic data in the context of the activities referred to in paragraphs (1) to (4) shall be restricted to persons acting under the authority of the service provider or operator and handling billing or traffic management, customer enquiries, fraud detection, marketing electronic communications services or providing a value added service. It must be restricted to what is necessary for the purposes of such activities.

(6) Any person who contravenes the provisions of paragraphs (1) to (5) of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.

Art. 5-1. *(Act of 24 July 2010)*

(1) "Data retained in accordance with articles 5 and 9 are subject to the conditions of articles 22 and 23 of the amended Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data.

(2) Data is deleted when the data retention period ends, with the exception of data that can be legally accessed and has been preserved.

Art. 5-2. (1) The National Commission for Data Protection provides the Commission of the European Union on a yearly basis with statistics on the retention of data in accordance with articles 5 and 9.
To this end, serivce providers and operators retain and transmit the information upon request to the National Commission, in particular:
- the cases in which information was provided to the competent authorities in accordance with applicable national law,
- the time elapsed between the date on which the data were retained and the date on which the competent authority requested the transmission of the data,
- the cases where requests for data could not be met.

(2) Such statistics shall not contain personal data."

Art. 6. Itemised billing

(1) Subscribers shall have the right to receive non-itemised bills free of charge.

(2) Free calls, including those made to help-lines, shall not be shown on any itemised bill, regardless of how detailed it is. In addition, an itemised bill shall not contain any indication enabling the person called to be identified.

Art. 7. Calling and connected line identification

(1) Where presentation of calling line identification is offered, the service provider shall enable the subscriber and the calling user to prevent, using a simple means and free of charge, the presentation of the calling line identification on a per-call

basis. The calling subscriber must at all times have this possibility on a per-line basis.

(2) Where presentation of calling line identification is offered, the called subscriber must be able, using a simple means and free of charge for reasonable use of that function, to prevent the presentation of the calling line identification of incoming calls.

(3) Where presentation of calling line identification is offered and where the calling line identification is presented prior to the call being established, the called subscriber must be able, using a simple means and free of charge, to reject incoming calls where the presentation of the calling line identification has been prevented by the calling user or subscriber.

(4) Where presentation of connected line identification is offered, the called subscriber must be able, using a simple means and free of charge, to prevent the presentation of the connected line identification to the calling user.
(Act of 28 July 2011)

(5)

(a) "Operators and providers of fix and mobile telephony services giving access to the single European emergency call number "112" and to the emergency call number specified by the Luxembourg Regulation Institute shall provide ("push") for every call to one of the emergency numbers the available data, including location data.
For the purposes of this paragraph, "available data" means:
- Identification data: the phone number, last name, first name(s), home or usual place of residence, corporate name or legal form of the company, place of establishment of the subscriber and the user if the latter is identified or identifiable; the indication if the data is public or not, as well as
- any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service (location data).

(b) The Luxembourg Regulation Institue determines, if needed, the technical modalities to make the data reffered to in paragraph (5) available."

(c) In the case of calls made to the single European emergency number 112 or the emergency numbers determined by the Institute, the calling line identification "and the location data of the caller" shall always be presented even where the caller has prevented it.

(d)

(6) The provisions of paragraph (1) shall also apply with regard to calls to third countries originating in the European Union. The provisions of paragraphs (2), (3) and (4) shall also apply to incoming calls originating in third countries.

(7) The service provider shall inform the public of the possibilities referred to above, by appropriate means and no later than the time when a contract is concluded.

(8) Any called subscriber claiming to be the victim of malevolent or obtrusive calls may request identification of the calling or connected line, and of repeated or inopportune calls declared to be malevolent or obtrusive which have been made or located on the basis of the same call number or connection. The detailed rules to be complied with by the service provider or operator, and by subscribers claiming to be the victims of malevolent or obtrusive calls, shall be laid down by Grand-Ducal regulation. That regulation shall also specify the characteristics of a malevolent or obtrusive call and shall prescribe the circumstances in which calling line identification may be used even where presentation thereof has been prevented.

(9) Any person who contravenes the provisions of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.

Art. 8. Automatic call forwarding

Where automatic call forwarding (or deviation) is offered, the service provider shall give each subscriber the possibility, using a simple means and free of charge, of

stopping automatic call forwarding by a third party to the subscriber's terminal where the service provider is able to identify the origin of the calls forwarded. Where appropriate, such identification shall be effected in collaboration with other service providers concerned.

Art. 9. Location data other than traffic data

(Act of 24 July 2010)

(1)

(a) "For the purposes of the investigation, detection and prosecution of criminal offences, subject to a criminal or correctional penalty of detention of up to one year, and solely with a view to enabling information to be made available, in so far as may be necessary, to the judicial authorities, any service provider or operator processing location data other than traffic data must retain such data for a period of 6 months from the date of the communication. The obligation to retain data shall include the retention of the data relating to unsuccessful call attempts where those data are generated or processed, and stored (as regards telephony data) or logged (as regards Internet data) in the process of supplying the communication services concerned. For the purpose of this paragraph, only one single location information is needed per communication or call. The categories of location data other than traffic data capable of being used for the investigation, detection and prosecution of criminal offences shall be determined by Grand-Ducal Regulation. This regulation shall also determine the forms and modalities according to which the data can be made available to the judicial authorities."

(b) Upon the expiry of the retention period provided for in (a) above, the service provider or operator shall be required to erase or render anonymous the location data other than traffic data relating to subscribers and users.

(Act of 24 July 2010)

(2) "Service providers or operators processing location data other than traffic data relating to subscribers and users shall be required to take all necessary steps to ensure the retention of such data for the period provided for in paragraph (1)(a) above, in such a way as to make it impossible for anyone to access the data in question with the exception of access which is ordered by authorities acting in the context of Article 67-1 of the Code of Criminal Procedure, or by authorities competent pursuant to Articles 88-1 to 88-4 of the Code of Criminal Procedure to safeguard State security, defence, public security and the prevention, investigation, detection and prosecution of criminal offences "referred to in paragraph (1) (a).""

(3) Service providers or operators may process location data other than traffic data relating to subscribers and users only if such data have been made anonymous or the subscriber or user concerned has given his/her consent thereto, to the extent and for the duration necessary for the supply of a value added service and subject to the provisions of paragraphs (2), (4) and (5).

(4) Service providers and, where appropriate, operators shall inform subscribers or users in advance of the types of location data other than traffic data processed, of the purposes and duration of the processing and whether the data will be transmitted to third parties for the purpose of providing the value added service. Subscribers or users shall be given the possibility to withdraw their consent to the processing of location data other than traffic data at any time. Where consent of the subscribers or users has been obtained for the processing of location data other than traffic data, the subscriber or user must continue to have the possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

(5) Processing of location data other than traffic data in the case of the activities referred to in paragraphs 1 to 4 shall be restricted to persons acting under the authority of the service provider or operator or of the third party providing the value added service, and must be restricted to what is necessary for such activities.

(6) Any person who contravenes the provisions of this article shall be liable to a term

of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.

Art. 10. Directories of subscribers

(1) Subscribers must be informed, free of charge and before they are included therein, about the purpose(s) of any printed or electronic directory of subscribers available to the public (hereinafter "the directory") or obtainable through directory enquiry services, in which their personal data can be included and of any further usage possibilities based on search functions embedded in electronic versions of the directory.

(2)
   (a) Subscribers must be given the opportunity of clearly indicating, upon taking out their subscription or at any other time when updates or new directories are published, whether their personal data are to be included in a public directory, and if so, which, to the extent that such data are relevant for the purpose of the directory as determined by the provider of the directory.
   (b) Subscribers must be able to verify, correct or withdraw such data. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it shall be free of charge.

(3) Any person who contravenes the provisions of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.

Art. 11. Unsolicited communications

(Act of 28 July 2011)

(1) “The use of automated calling and communication systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may be allowed only in respect of subscribers or users who have given their prior consent.”

(2) Notwithstanding paragraph (1), where a supplier obtains from its customers their electronic contact details for electronic mail, in the context of the sale of a product or a service, that supplier may use those electronic contact details for direct marketing of its own similar products or services provided that customers are clearly and distinctly given the opportunity to object, free of charge and in an easy manner, to such use of electronic contact details when they are collected and on the occasion of each message where the customer has not initially refused such use.

(3) The transmission of unsolicited communications for purposes of direct marketing by means other than those referred to in paragraphs 1 and 2 shall be permissible only with the prior consent of the subscriber “or user” concerned.

(4) The practice of sending electronic mail for purposes of direct marketing disguising, concealing or misrepresenting the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease, is prohibited.

(5) Paragraphs (1) and (3) shall apply to subscribers who are natural persons.

(6) Any person who contravenes the provisions of this article shall be liable to a term of imprisonment lasting between eight days and one year and/or a fine of between 251 and 125 000 euros. The court seised of the matter may order the cessation of any processing which contravenes the provisions of this article, on pain of a periodic pecuniary penalty in a maximum sum to be fixed by the court in question.

Art. 12. National Commission for Data Protection

The National Commission for Data Protection set up by Article 32 of the Act of 2 August 2002 on the protection of persons with regard to the processing of personal

data shall be responsible for the application of the provisions of this Act and of the regulations enacted for the implementation thereof *(Act of 2 August 2002)* “without prejudice to the application of Article 8 of the amended Act of 2 August 2002 on the protection of persons with regard to the processing of personal data).”

Art. 13. Transitional provision

Any supplier providing a public directory within the meaning of Article 10 prior to the entry into force of this Act shall inform the subscribers, without delay and in accordance with Article 10(1), of the purpose for which their data are processed.

Art.14. Amending provisions

The following articles of the Code of Criminal Procedure are hereby amended as follows:

(a) Art. 88-2: paragraphs 1, 2, 3 and 5 of Article 88-2 of the Code of Criminal Procedure are amended as follows:

Paragraph 1: Decisions by the juge d'instruction [investigating judge] or the President of the judges' chambers of the Cour d'Appel [Court of Appeal] ordering the surveillance and monitoring of telecommunications or of mail entrusted to the postal system shall be notified to the operators of the postal or telecommunications systems, who shall cause the same to be implemented without delay.

Paragraph 2: Such decisions, and any steps taken to implement them, shall be entered in a special register maintained by each the postal or telecommunications operator.

Paragraph 3: Any telecommunications recorded and items of correspondence, data or information obtained by other technical means of surveillance and monitoring pursuant to Article 88-1 shall be forwarded, duly sealed and in return for a valid receipt, to the juge d'instruction [investigating judge], who shall draw up an official record of their delivery to him. He shall cause copies to be made of any correspondence which may help to secure a conviction or discharge, and shall file those copies, together with the recordings and all other data and information received, in the official file. He shall return all documents which in his view do not need to be retained to the postal operators, who shall forward them without delay to the addressee.

Paragraph 5: Communications with persons who are bound by professional secrecy, within the meaning of Article 458 of the Criminal Code, and who are not suspected themselves of having committed or participated in the offence, may not be used. All recordings and transcriptions thereof shall be destroyed forthwith by the juge d'instruction [investigating judge].

(b) Art. 88-4: paragraphs 1 and 4 of Article 88-4 of the Code of Criminal Procedure are amended as follows:

Paragraph 1: Decisions of the Head of the Government ordering the surveillance and monitoring of telecommunications or of correspondence shall be notified to the postal or telecommunications operators, who shall cause the same to be implemented without delay.

Paragraph 4: The items of correspondence shall be forwarded, duly sealed and in return for a valid receipt, to the Intelligence Service. The Head of the Service shall cause copies to be made of any correspondence which may help to secure a conviction or discharge, and shall return all documents which in his view do not need to be retained to the postal operators, who shall forward them to the addressee.

Art. 15. Miscellaneous provision

The present Act may be referred to in a shortened form as follows: *"Act of 30 May 2005 on the protection of privacy in the electronic communications sector"*.

Art. 16. Entry into force

This Act shall enter into force on the first day of the month following its publication in the Mémorial [Official Gazette].

We command and order that this Act be included in the Mémorial [Official Gazette], so that it may be implemented and complied with by all persons whom it may concern.