MEMORIAL *Unofficial English translation*

Official Journal of the Grand Duchy of Luxembourg

Compendium of legislation

A — Number 73 7th of June 2005

Law 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

We, Henri, Grand Duke of Luxembourg, Duke of Nassau,

Having consulted our State Council,

With the assent of the Chamber of Deputies,

Having regard to the decision of the Chamber of Deputies of 28 April 2005 and that of the State Council of 24 May 2005 specifying that there is no need for a second vote in the matter,

Have ordered, and hereby order, as follows:

Article 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.

Article 2 – Definitions

For the purposes of this Law:

(a) "subscriber" means a natural or legal person who or which is party to a contract with an undertaking offering publicly available electronic communication services for the supply of such services;

(b) "call" means a connection established by means of a publicly available telephone service allowing two-way communication in real time;

(c) "consent" means any freely given specific and informed indication of his wishes by which the person concerned or his legal, judicial or statutory representative signifies his agreement to personal data relating to him being processed;

(d) "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;

(e) "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;

(f) "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;

(g) "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;

(h) "Institute" means the Institut Luxembourgeois de Régulation [Luxembourg Regulation Institute];

(i) "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;

(j) "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";

(k) "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";

(l) "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;

(m) "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.

Article 3 – Security

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.

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.

Article 4 – Confidentiality of communications

1. Each service provider or operator shall ensure the confidentiality of communications, and of the traffic data relating thereto, effected by means of a public communications network and publicly available electronic communications services.

2. No person other than the user concerned may listen to, tap or store communications or the traffic data relating thereto, or engage in any other kinds of interception or surveillance thereof, without the consent of the user concerned.

3. Paragraph 2:

(a) shall not preclude technical storage which is necessary for the conveyance of a communication, without prejudice to the principle of confidentiality;

(b) shall not apply to authorities acting in the context of a serious offence in the course of its commission or immediately thereafter, or in the context of Article 40 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 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;

(e) shall not apply where electronic communications networks are used with a view to storing information or accessing information stored in a subscriber's or user's terminal equipment by means of "cookies" or similar devices, provided that such "cookies" or devices are used for legitimate purposes, that the subscriber or user is provided with clear and full information, *inter alia* regarding the purpose of the processing, and that the subscriber or user has the right to object to such processing by the processor.
This provision shall not preclude storage or technical 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.

Article 5 – Traffic data

1.(a) For the purposes of the investigation, detection and prosecution of criminal offences, 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 12 months. 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:

– ordered by authorities acting in the context of a serious offence in the course of its commission or immediately thereafter, or in the context of Article 40 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 six 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.

Article 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.

Article 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.

5. 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 shall always be presented even where the caller has prevented it.

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.

Article 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.

Article 9 – Location data other than traffic data

1.(a) For the purposes of the investigation, detection and prosecution of criminal offences, 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 12 months. For the application of this paragraph, one single item of location information shall be required 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. The location data other than traffic data shall also be communicated to the single European emergency number 112 and to the emergency numbers determined by the Institute.

(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.

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 a serious offence in the course of its commission or immediately thereafter, or in the context of Article 40 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.

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.

Article 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.
Article 11 – Unsolicited communications

1. The use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of

direct marketing is permissible only in respect of subscribers 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 concerned.

4. The practice of sending of 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.

Article 12 – National Data Protection Commission

The National Data Protection Commission set up by Article 32 of the Law 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 Law and of the regulations enacted for the implementation thereof.

Article 13 – Transitional provision

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

Article 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.

Article 15 – Miscellaneous provision

The present Law may be referred to in a shortened form as follows: "Law of ... on the protection of privacy in the electronic communications sector".

Article 16 – Entry into force

This Law 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 Law be included in the *Mémorial* [Official Gazette], so that it may be implemented and complied with by all persons whom it may concern.

Jean-Louis Schiltz, Minister of State for Communications
Palace of Luxembourg, 30 May 2005. Henri
Luc Frieden, Minister of Justice

Parl. doc. 5181, ordinary sessions 2002-2003, 2003-2004, 2nd extraordinary session 2004, ordinary session 2004-2005; Dir. 2002/58/EC.