SUBSIDIARY LEGISLATION 440.01

PROCESSING OF PERSONAL DATA (ELECTRONIC COMMUNICATIONS SECTOR) REGULATIONS

15th July, 2003

LEGAL NOTICE 16 of 2003, as amended by Legal Notices 153 of 2003, 522 of 2004, 109 of 2005, 426 of 2007, 198 of 2008, 239 of 2011 and 429 of 2013.

Citation.
Amended by: L.N. 522 of 2004; L.N. 429 of 2013.

1. (1) The title of these regulations is the Processing of Personal Data (Electronic Communications Sector) Regulations.

(2) These regulations implement the provisions of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (directive on privacy and electronic communications), as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

(3) These regulations also implement, and are to be read in conjunction with, the requirements of Commission Regulation (EU) No 611/2013 of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications.

Definitions.
Amended by: L.N. 522 of 2004; L.N. 239 of 2011.
Cap, 399.
Cap. 440.

2. (1) Unless otherwise stated in these regulations, the definitions in the Electronic Communications (Regulation) Act and the Data Protection Act shall apply.

(2) In these regulations, unless the context otherwise requires:

Cap. 440.

"Act" unless otherwise stated in these regulations, means the Data Protection Act;

"Authority" means the Malta Communications Authority;

"Commissioner" means the Data Protection Commissioner;

"communication" means any information exchanged or transmitted 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 a electronic communications network except to the extent that the information can be related to the identifiable subscriber or user receiving the information;

"consent" means consent by a user or subscriber and corresponds to the consent given by a data subject in accordance with article 2 of the Act;

"controller" means the controller of personal data and shall have the same meaning as under the Act;

"directory of subscribers" or "directory" means a directory of subscribers to publicly available electronic communications services, whether in printed form or in electronic form -

(*a*) which is available to the public or a section of the public, or

(*b*) information which is normally provided by a directory enquiry service;

"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;

"information society service" shall have the same meaning as under the Electronic Commerce Act; Cap. 426.

"location data" means any data processed in an electronic communications network or by an electronic communication service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service;

"Minister" unless otherwise stated in these regulations means the Minister responsible for data protection;

"person" includes any body corporate and any body of persons whether or not it has a legal personality distinct from that of its members;

"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;

"processing" and "processing of personal data" mean any operation or set of operations which is taken in regard to personal data, whether or not it occurs by automatic means, and includes the collection, recording, organisation, storage, adaptation, alteration, retrieval, gathering, use, disclosure by transmission, dissemination or otherwise making information available, alignment or combination, blocking, erasure or destruction of such data;

"traffic data" means any data processed for the purpose of the conveyance of a communication on a electronic communications network or for the billing thereof;

"user" means any natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to such service;

"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.

PART I - Processing of Personal Data

Added by: L.N. 198 of 2008.

Application. *Amended by: L.N. 522 of 2004; L.N. 239 of 2011.*

3. These regulations shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in Malta and any other country, including public communications networks supporting data collection and identification devices, as the Minister may after consultation with the Minister responsible for communications, designate by notice in the Gazette.

Security of processing. *Added by: L.N. 239 of 2011.*

3A. (1) 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 Commissioner.

(2) 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.

(3) 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 Commissioner that he 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.

(4) 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 Commissioner, having considered the likely adverse effects of the breach, may require him to do so.

(5) The notification to the subscriber or individual shall at least include 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 Commissioner shall, in addition, include the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

(6) The Commissioner shall encourage the drawing up of 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 has to be made.

(7) Service 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 Commissioner to verify compliance with the provisions of this regulation.

Confidentiality of communications.

4. (1) Without prejudice to regulation 10 no person other than the user, shall listen, tap, store or undertake any other form of interception or surveillance of communications and of any related traffic data, without the consent of the user concerned.

(2) This regulation shall not affect any legally authorised recording of communications and the related traffic data in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

Access to information stored in terminal equipment.
Amended by: L.N. 522 of 2004. Substituted by: L.N. 239 of 2011.

5. (1) The storing of information or the gaining of access to information 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 consent, having been provided by the controller with clear and comprehensive information in terms of article 19 of the Act.

(2) The requirements contained in this regulation shall not prevent the 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 may be strictly necessary in order for the service provider to provide an information society service explicitly requested by the subscriber or user to provide the service.

Traffic data.
Amended by: L.N. 522 of 2004.

6. (1) Without prejudice to sub-regulations (2), (3) and (4), traffic data relating to subscribers and users processed for the purpose of the transmission of a communication and stored by a undertaking which provides publicly available electronic communications services or by an undertaking which provides a public communications network shall be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.

(2) Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed provided that such processing shall only be permissible up to the end of the period during which the bill may lawfully be challenged or payment pursued.

(3) For the purpose of marketing its own electronic communications services or for the provision of value added services to the subscriber, the undertaking which provides publicly available electronic communications services may process the data referred to in sub-regulation (1) to the extent and for the duration necessary for such services, provided the subscriber has given his consent.

(4) The undertaking which provides publicly available electronic communications services shall inform the subscriber or user of the types of traffic data that are processed and of the duration of such processing for the purposes mentioned in sub-regulation (2) and, prior to obtaining consent, for the purposes

mentioned in sub-regulation (3).

(5) Processing of traffic data in accordance with sub-regulations (1) to (4) shall be restricted to persons acting under the authority of the undertakings which provides publicly available electronic communications and of the undertakings which provide a public communications network handling billing or traffic management, customer enquiries, fraud detection, marketing the electronic communications services of the provider or providing a value added service, and shall be restricted to what is necessary for the purposes of such activities.

(6) Nothing in this regulation shall preclude the furnishing of traffic data to any competent authority for the purposes of any law relating to the settling of disputes, in particular interconnection and billing disputes.

Location data.
Amended by:
L.N. 522 of 2004.

7. (1) Where location data other than traffic data, relating to users or subscribers of public communications networks or of publicly available electronic communications services can be processed, such data may only be processed when it is made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service.

(2) Prior to obtaining the consent of the users or subscribers, the undertaking which provides publicly available electronic communications services shall inform them of the following:

(*a*) the type of location data other than traffic data, which shall be processed,

(*b*) the purposes and duration of the processing, and

(*c*) whether the data shall be transmitted to a third party for the purpose of providing the value added service:

Provided that at any time users or subscribers may withdraw their consent for the processing of location data other than traffic data.

(3) Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber shall 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.

(4) The processing of location data other than traffic data in accordance with sub-regulations (1), (2) and (3) shall be restricted to persons acting under the authority of the undertaking which provides publicly available electronic communications services or of the undertaking which provides a public communications network or of the third party providing the value added service, and shall be restricted to what is necessary for the purposes of providing the value added service.

Directory of subscribers.

8. (1) Any person who produces a directory of subscribers shall, without charge to the subscriber and before any personal data relating to the subscriber is included in the directory, ensure that -

(*a*) the subscriber is informed about the purposes of such a directory of subscribers and of any usage possibilities based on search functions embedded in the electronic version of the directory;

(*b*) no personal data are included in such a directory without the consent of the subscriber. In giving his consent the subscriber shall determine which data is to be included in the directory, to the extent that such data is relevant for the purpose of the directory as determined by the provider of the directory service. Subscribers shall be given the opportunity to verify, correct or withdraw such personal data from the directory; and

(*c*) the personal data in such a directory relating to a subscriber is limited to what is necessary to identify the subscriber and the number allocated to him, unless the subscriber has given his additional consent to the provider of the directory service authorising him to include in the directory additional personal data of the subscriber:

Provided that the above shall apply only to subscribers who are natural persons.

(2) This regulation shall not apply to an edition of a directory that has been already produced or placed on the market in printed or off-line electronic form before the coming into force of these regulations.

(3) Where the personal data of subscribers to fixed or mobile public voice telephony services has been included in a public subscriber directory before the coming into force of these regulations, the personal data of such subscribers may remain in this public directory in its printed or electronic versions, including versions with reverse search functions, unless subscribers indicate otherwise, after having received complete information from the provider of the directory services about the purposes and options in accordance with this regulation.

Unsolicited communications. *Amended by: L.N. 522 of 2004; L.N. 109 of 2005. Substituted by: L.N. 239 of 2011.*

9. (1) A person shall not use, or cause to be used, any publicly available electronic communications service to make an unsolicited communication for the purpose of direct marketing by means of -

(*a*) an automatic calling machine; or

(*b*) a facsimile machine; or

(*c*) electronic mail,

to a subscriber or user, irrespective of whether such subscriber or user is a natural person or legal person, unless the subscriber or user has given his prior consent in writing to the receipt of such a communication.

(2) Notwithstanding sub-regulation (1), where a person has obtained from his customers their contact details for electronic mail in relation to the sale of a product or a service, in accordance with

the Act, that same person may use such details for direct marketing of its own similar products or services:

Provided that customers shall be given the opportunity to object, free of charge and in an easy and simple manner, to such use of electronic contact details at the time of their collection and on the occasion of each message where the customer has not initially refused such use.

(3) A person who uses or causes to be used any other means of communication other than those stated in sub-regulations (1) and (2) for the purpose of direct marketing shall, at no charge to the subscriber or user, ensure that any such communications to a subscriber or user are not sent if the subscriber or user requests that such communications cease.

(4) In all cases the practice of sending electronic mail for the purposes of direct marketing disguising or concealing the identity of the sender on whose behalf the communication is made, which contravene the provisions of regulation 6 of the Electronic Commerce (General) Regulations, or 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 such regulation, shall be prohibited. S.L. 426.02

Non-applicability of certain regulations.

10. The provisions of regulations 4, 5, 6 and 7 shall not apply when a law specifically provides for the provision of information as a necessary measure in the interest of:

(*a*) national security;

(*b*) defence;

(*c*) public security;

(*d*) the prevention, investigation, detection and prosecution of criminal or administrative offences, or of breaches of ethics for regulated professions;

(*e*) an important economic or financial interest including monetary, budgetary and taxation matters;

(*f*) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority referred to in paragraphs (*c*), (*d*) and (*e*); or

(*g*) the protection of the subscriber or user or of the rights and freedoms of others.

Compensation for failure to comply with regulations.

11. (1) A person who suffers any loss or damage because of any contravention of these regulations by any other person shall be entitled to take action before the competent court seeking compensation from that other person for that loss or damage.

(2) The period of limitation provided for in article 46 (2) of the Act shall apply to an action under sub-regulation (1).

Enforcement.

12. The Commissioner shall ensure compliance with the provisions of these regulations.

Administrative fines and sanctions. *Amended by L.N. 153 of 2003; L.N. 426 of 2007.*

13. Any person who contravenes or fails to comply with these regulations shall be liable to an administrative fine not exceeding twenty-three thousand and two hundred and ninety-three euro and seventy-three cents (23,293.73) for each violation and two thousand and three hundred and twenty-nine euro and thirty seven cents (2,329.37) for each day during which such violation persists, which fine shall be determined and imposed by the Commissioner.

Appeals from decisions of the Commissioner.

14. Any person aggrieved by a decision taken by the Commissioner in accordance with these regulations and having a legal interest to contest such a decision may appeal to the Data Protection Appeals Tribunal.

Advice and consultation with the Authority.

15. The Commissioner may seek the advice of, and shall where appropriate consult with, the Authority in the exercise of his functions under these regulations.

Request that the Commissioner exercise his enforcement functions.

16. Where it is alleged that any of these regulations have been contravened, the Authority or any aggrieved person may request the Commissioner to exercise his enforcement functions in respect of that contravention:

Provided that nothing in this regulation shall be interpreted as a limitation on the discretionary powers of the Commissioner.

Added by: L.N. 198 of 2008.

Part II – Retention of Data

Definitions. *Added by: L.N. 198 of 2008.*

17. In this Part, unless the context otherwise requires -

"cell ID" means the identity of the cell from which a mobile telephony call originated or in which it terminated;

"data" means traffic data and location data and the related data necessary to identify the subscriber or user;

"Police" means the Commissioner of Police and includes any officer of the Police designated by the Commissioner to act on his behalf;

Cap. 391.

"security service" means the Security Service as defined in the Security Service Act;

"serious crime" means any crime which is punishable by a term of imprisonment of not less than one year and for the purposes of these regulations includes the crimes mentioned in articles 48(1)(*d*) and 49 of the Electronic Communications (Regulation) Act;

Cap. 399.

"subscriber" means any natural or legal person who is party to a contract with the provider of publicly available electronic communications services or of a public communications network, for the supply of such services, and includes a pre-paid customer of such provider;

"telephone service" means calls (including voice, voicemail and conference and data calls), supplementary services (including call forwarding and call transfer) and messaging and multi-media services (including short message services, enhanced media services and multi-media services);

"unsuccessful call attempt" means a communication where a

telephone call has been successfully connected but not answered or there has been a network management intervention;

"user" means any legal entity or natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to that service;

"user ID" means a unique identifier allocated to persons when they subscribe to or register with an Internet access service or Internet communications service.

Obligation to retain data.
Added by: L.N. 198 of 2008.

18. (1) Notwithstanding the provisions of regulations 4, 5, 6 and 7, a service provider of publicly available electronic communications services or of a public communications network shall retain the data specified in regulation 20 to the extent that those data are generated or processed by such providers in the process of supplying the communications services concerned.

(2) The obligation to retain the data as provided in sub-regulation (1) shall, to the extent that such data are generated or processed, and stored (as regards telephony data) or logged (as regards internet data) be applicable to unsuccessful call attempts:

Provided that such obligation shall not be applicable in relation to unconnected calls.

(3) No data revealing the content of any communication may be retained pursuant to these regulations.

Access to data.
Added by: L.N. 198 of 2008.

19. (1) Data retained under this Part shall be disclosed only to the Police or to the Security Service, as the case may be, where such data is required for the purpose of the investigation, detection or prosecution of serious crime.

(2) When data retained under this Part is required, such data shall be provided by a service provider of publicly available electronic communications services or of a public communications network, from whom it is required, in an intelligible form and in such a way that it is visible and legible.

(3) A request for data shall be made in writing and shall be clear and specific:

Provided that where the data is urgently required, such request may be made orally, so however that the written request shall be made at the earliest opportunity.

(4) Data retained under this Part shall, following the request, be provided without undue delay.

Categories of data to be retained.
Added by: L.N. 198 of 2008.

20. Service Providers are required to retain the following categories of data:

(1) data necessary to trace and identify the source of a communication:

(*a*) concerning fixed network telephony and mobile telephony:

(i) the calling telephone number;

(ii) the name and address of the subscriber or registered user;

(*b*) concerning Internet access, Internet e-mail and Internet telephony:

(i) the user ID allocated;

(ii) the used ID telephone number allocated to any communication entering the public telephone network;

(iii) the name and address of the subscriber or registered user to whom an Internet-Protocol address, user ID or telephone number was allocated at the time of the communication;

(2) data necessary to identify the destination of a communication:

(*a*) concerning fixed network telephony and mobile telephony:

(i) the telephone number or numbers dialled or called and, in cases involving supplementary services such as call forwarding or call transfer, the number, or numbers to which the call is routed;

(ii) the name and address of the subscriber or registered user;

(*b*) concerning Internet e-mail and Internet telephony:

(i) the user ID or telephone number of the intended recipient of an Internet telephony call;

(ii) the name and address of the subscriber or registered user and user ID of the intended recipient of the communications;

(3) data necessary to identify the date, time and duration of a communication:

(*a*) concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;

(*b*) concerning Internet access, Internet e-mail and Internet telephony:

(i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the Internet Protocol address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

(ii) the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone;

(4) data necessary to identify the type of communication:

(*a*) concerning fixed network telephony and mobile telephony, the telephone service used;

(*b*) concerning Internet e-mail and Internet telephony, the Internet service used;

(5) data necessary to identify users' communication equipment or what purports to be their equipment:

(*a*) concerning fixed network telephony, the calling and called telephone numbers;

(*b*) concerning mobile telephony:

(i) the calling and called telephone numbers;

(ii) the International Mobile Subscriber Identity of the calling party;

(iii) the International Mobile Equipment Identity of the calling party;

(iv) the International Mobile Subscriber Identity of the called party;

(v) the International Mobile Equipment Identity of the called party;

(vi) in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the services was activated;

(*c*) concerning Internet access, Internet e-mail and Internet telephony:

(i) the calling telephone numbers for dial-up access;

(ii) the digital subscriber line or other end point of the originator of the communication;

(6) data necessary to identify the location of mobile communication equipment:

(*a*) the location label (Cell ID) at the start of the communication;

(*b*) data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained.

Periods of retention.
Added by: L.N. 198 of 2008.

21. The categories of data specified in regulation 20 shall be retained by the service providers for the following periods:

(*a*) communications data relating to Internet Access and Internet e-mail for a period of six months from the date of communication;

(*b*) communications data concerning fixed network telephony, mobile telephony and Internet telephony for a period of one year from the date of communication.

Conservation order.
Added by: L.N. 198 of 2008.

22. (1) The Police may, in addition to the request for data under regulation 19, issue a conservation order in relation to the data.

(2) The conservation order shall be served on the service provider within the retention period applicable under regulation 21.

(3) Where a conservation order has been issued, the service provider shall conserve the data -

(*a*) either for a period of six months in addition to the original or extended applicable retention period which period shall not, without an order of a Magistrate or of a competent Court, exceed a total period of two years; or

(*b*) where criminal proceedings have been commenced within the applicable retention period or within such period as extended in accordance with paragraph (*a*), for such time as may be necessary for the conclusion of the criminal proceedings where the data is required to be produced as evidence; such conclusion shall be deemed to occur when the judgement in the proceedings becomes final and conclusive, whichever is the longer period.

Data security. *Added by: L.N. 198 of 2008.*

23. Data retained under this Part shall comply with the data security principles established under the Act and shall as a minimum -

(*a*) be of the same quality and subject to the same security and protection as the data on the network;

(*b*) be subject to appropriate technical and organisational measures to protect the data against accidental or unlawful destruction, accidental loss or alteration, or unlawful storage, processing, access or disclosure;

(*c*) be subject to appropriate technical and organisational measures to ensure that they can be accessed by specially authorised personnel only;

(*d*) except for such data as are the subject of a conservation order, be destroyed at the end of the applicable retention period.

Statistics. *Added by: L.N. 198 of 2008.*

24. (1) Service providers shall, in relation to the retention of data under this Part, provide on an annual basis, the following information to the Data Protection Commissioner -

(*a*) the cases in which information was provided under this Part;

(*b*) the time elapsed between the date on which the data were retained and the date on which the transmission of the data was requested;

(*c*) any cases where requests for data could not have been met.

(2) Any statistics provided under this regulation shall not contain any personal data.