

NB: Unofficial translation

© Ministry of Transport and Communications of Finland

Act on the Protection of Privacy in Electronic Communications

(516/2004)

Chapter 1 – **General provisions**

Section 1 – *Objective of the Act*

The objective of the Act is to ensure confidentiality and protection of privacy in electronic communications and to promote information security in electronic communications and the balanced development of a wide range of electronic communications services.

Section 2 – *Definitions*

For the purposes of this Act:

- 1) *message* means a phone call, e-mail message, SMS message, voice message or any comparable message transmitted between parties or to unspecified recipients in a communications network;
- 2) *communications network* means a system comprising cables and equipment joined to each other for the purpose of transmitting or distributing messages by wire, radio waves, optically or by other electromagnetic means;
- 3) *public communications network* means a communications network available to a set of users that is not subject to any prior restriction;
- 4) *telecommunications operator* means a network operator or service operator as referred to in

sections 2(17) and 2(19), respectively, of the Communications Market Act (393/2003);

- 5) *network service* means the provision of a communications network by a telecommunications operator for the purposes of transmitting, distributing or providing messages to a set of users that is not subject to any prior restriction;
- 6) *communications service* means the transmission, distribution or provision of messages by a telecommunications operator in a communications network to a set of users that is not subject to any prior restriction;
- 7) *value added service* means a service based on the processing of identification data or location data for a purpose other than the provision of a network service or communications service;
- 8) *identification data* means data which can be associated with a subscriber or user and which is processed in communications networks for the purposes of transmitting, distributing or providing messages;
- 9) *location data* means data which shows the geographic location of a subscriber connection or terminal device and which is used for a purpose other than the provision of a network service or communications service;
- 10) *subscriber* means a legal person or a natural person who has entered into an agreement concerning the provision of a communications service or a value added service;
- 11) *corporate or association subscriber* means a company or organization which subscribes (to) a communications service or a value added service and which processes users' confidential messages, identification data or location data in its communications network;

- 12) *user* means a natural person who uses a communications service or a value added service without necessarily being a subscriber to the service;
- 13) *information security* means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, that data can only be modified by those who are entitled to do so, and that data systems can be used by those who are entitled to use them; and
- 14) *processing* means collecting, saving, organizing, using, transferring, disclosing, storing, modifying, combining, protecting, removing, destroying and other similar actions.

Section 3 – *Scope of application*

- (1) This Act applies to network services, communications services, value added services and services where data describing the use of the service is processed, which are provided in public communications networks. This Act also applies to direct marketing in public communications networks and to subscriber directory services and telephone directory services.
- (2) This Act does not apply to internal communications networks and other communications networks accessible to a restricted set of users, unless such networks are connected to a public communications network referred to in subsection 1.
- (3) Notwithstanding the above, sections 4 and 5 of this Act apply to internal communications networks and other communications networks accessible to a restricted set of users, even if such networks are not connected to a public communications network referred to in subsection 1.

- (4) Unless otherwise provided in this Act, the Personal Data Act (523/1999) applies to the processing of personal data.
- (5) The relationship between an employer and an employee is also subject to the provisions of the Act on the Protection of Privacy in Working Life (477/2001).
- (6) This Act does not apply to messages transmitted over a mass communications network if the message cannot be associated with an individual case of a subscriber or user receiving it.
- (7) This Act does not apply to the actions of public authorities in public authority networks as defined in the Communications Market Act or in any other communications network built for the needs of public order and security, national defence, rescue operations, civil defence or the safety of land, sea, rail or air transport.
- (8) This Act does not apply in cases where the Act on Preventing and Clearing Money Laundering (68/1998) provides otherwise.

Chapter 2 – **Protection of privacy and confidentiality of messages**

Section 4 – *Confidentiality of messages, identification data and location data*

- (1) All messages, identification data and location data are confidential unless this Act or another Act provides otherwise.

- (2) A message is not confidential if it has been transmitted to be universally received. However, the identification data associated with such a message is confidential. Provisions on disclosing the identification data of a network message are laid down in section 17 of the Act on the Exercise of Freedom of Expression in Mass Media (460/2003).
- (3) Subsection 1 above also applies to identification data generated through the browsing of websites.

Section 5 – *Obligation of secrecy and non-exploitation*

- (1) Whoever receives or obtains in any other way knowledge of a confidential message or identification data not intended for him or her must not disclose or make use of the content or identification data of such a message, or the knowledge of its existence, without the consent of a party to the communication, unless otherwise provided by law.
- (2) Whoever receives or obtains in any other way knowledge of location data not intended for him or her must not disclose or make use of the data, or the knowledge of its existence, without the consent of the party to whom the data applies, unless otherwise provided by law.
- (3) Current and former employees of a telecommunications operator, value added service provider, corporate or association subscriber or telecommunications contractor referred to in section 137 of the Communications Market Act must not disclose knowledge obtained through their employment about messages, identification data and location data without the consent of a party to the communication or the party to whom the location data applies, unless otherwise provided by law.

- (4) The obligation of secrecy referred to in subsection 3 above also covers all persons who are or have been acting on behalf of a telecommunications operator, value added service provider, corporate or association subscriber or telecommunications contractor.

Section 6 – *Protecting messages and identification data*

- (1) Subscribers and users may protect their messages and identification data in any way they wish, using any technical means available for the purpose, unless otherwise provided by law. Implementation of such protection must not interfere with the provision or use of any network service or communications service.
- (2) The possession, importing, manufacture and distribution of any system or part thereof for decoding the technical protection of electronic communications is prohibited in cases where such a system or part thereof is primarily intended for unlawful decoding of technical protection.
- (3) The Finnish Communications Regulatory Authority may, if there is an acceptable reason, grant an exception to the provision of subsection 2.

Section 7 – *Saving data on the use of a service in the user's terminal device and the use of such data*

- (1) The service provider may, by means of a communications network, save cookies or other data on the use of a service in the user's terminal device and use such data if the service provider gives the user comprehensible and complete information on the purpose of saving or using such data. The user must

also be given the opportunity to prohibit the saving and use referred to in this subsection.

- (2) The service provider's obligation to give information and the user's right to prohibit the use of data as referred to in subsection 1 above does not apply to any saving or use of data which is intended solely for the purpose of enabling or facilitating the transmission of messages in communications networks or which is necessary for the purpose of providing a service that the subscriber or user has specifically requested.
- (3) The saving and use of data referred to above in this section is allowed only to the extent required for the service, and it may not encroach on the protection or privacy any more than is necessary.

Chapter 3 – **Processing of messages and identification data**

Section 8 – *General processing provisions*

- (1) The sender and intended recipient of a message are entitled to process their own messages and the identification data associated with these messages unless otherwise provided below in this Act or in any other Act.
- (2) Confidential messages and identification data may be processed with the consent of the sender or intended recipient of such a message or if so provided by law.
- (3) Processing as referred to in sections 9-14 below is only allowed to the extent necessary for the purpose of such processing, and it may not encroach on the confidentiality of messages or the protection of

privacy any more than is necessary. Identification data may only be disclosed to those parties entitled to process it in the given situation. After processing, messages and identification data must be destroyed or rendered such that they cannot be associated with the subscriber or user involved, unless otherwise provided by law.

Section 9 – Processing identification data for the purpose of providing and using services

- (1) Identification data may only be processed to the extent necessary for the purpose of the provision and use of a network service, communications service or value added service and for the purpose of ensuring information security in these services.
- (2) Identification data may only be processed by a natural person employed by or acting on behalf of a telecommunications operator, value added service provider or corporate or association subscriber for the purpose of processing data to perform the functions referred to separately in subsection 1 and sections 10-14.

Section 10 – Processing for billing purposes

- (1) Telecommunications operators and value added service providers may process identification data necessary for defining fees between themselves and for billing purposes.
- (2) A corporate or association subscriber may process identification data necessary for internal billing.
- (3) An information society service provider as defined in the Act on the Provision of Information Society Services (458/2002) may process identification data

received from a telecommunications operator which is necessary for the billing of image recordings, sound recordings and other fee-based services offered over a communications network administered by that telecommunications operator, and any other data necessary for billing, if the subscriber or user to whom the data applies has given his or her consent thereto.

- (4) Information society service providers are entitled to obtain the data referred to in subsection 3 from telecommunications operators. The provisions of this Chapter and Chapters 2, 4 and 5 regarding the confidentiality of communications, the protection of privacy, the processing of messages and identification data, the processing of location data and information security in communications with regard to value added service providers apply to the recipient of such disclosed data.
- (5) Billing-related data must be stored for a minimum of three months from the due date of the bill or the saving of the identification data, whichever is later. Such data must not, however, be stored beyond the time the debt becomes statute-barred under the Act on statute-barred debt (728/2003). However, in the case of a dispute over a bill, the data pertaining to that bill must be stored until the matter has been settled or resolved.
- (6) Telecommunications operators and value added service providers must inform subscribers or users about what identification data is being processed and how long the processing will last.

Section 11 – *Processing for marketing purposes*

- (1) A telecommunications operator may, for the purpose of marketing communications services or value added services, process identification data to such an extent and for such a period of time as the marketing requires if the subscriber or user to whom the data applies has given his or her consent thereto.
- (2) Telecommunications operators must, prior to obtaining consent, inform subscribers or users about what identification data is to be processed and how long the processing would last.
- (3) The party giving such consent must have the opportunity to cancel his or her consent regarding the processing of identification data.

Section 12 – *Processing for the purposes of technical development*

- (1) Telecommunications operators and value added service providers may process identification data for the purposes of technical development of services.
- (2) Telecommunications operators and value added service providers must, prior to beginning the processing referred to in subsection 1 above, inform subscribers or users about what identification data is to be processed and how long the processing will last.
- (3) A corporate or association subscriber may process identification data for the purpose of technical development of its own activities

Section 13 – *Processing in cases of misuse*

A telecommunications operator, value added service provider or corporate or association subscriber may process identification data if this is necessary to detect, prevent, investigate and commit to pre-trial investigation any non-paying use of fee-based network services, communications services or value added services, or any similar cases of misuse.

Section 14 – *Processing for the purpose of detecting a technical fault or error*

A telecommunications provider, value added service provider or corporate or association subscriber may process identification data if this is necessary for the purpose of detecting a technical fault or error in the transmission of communications.

Section 15 – *Saving information on processing*

- (1) A telecommunications provider must save detailed event log information on any processing of identification data. This event information must show the time and duration of the processing and the person performing the processing. The event information must be stored for two years from the date on which it was saved.
- (2) The Finnish Communications Regulatory Authority may issue further regulations on the technical implementation of the saving and storing referred to in subsection 1.

Chapter 4 – **Location data**

Section 16 – *Processing and disclosure of location data*

- (1) Telecommunications operators, value added service providers and corporate or association subscribers and any persons acting on their behalf may process location data subject to the provisions of this Chapter for the purpose of providing and using value added services. However, the provisions of this Chapter do not, unless otherwise provided by law, apply to location data rendered such that it cannot, in itself or in combination with other data, be associated with a specific subscriber or user.
- (2) Processing of location data must be restricted to persons employed by or acting on behalf of the telecommunications operator, value added service provider or corporate or association subscriber whose job involves the processing of location data for the purpose of carrying out measures referred to in this Chapter.
- (3) Such processing is allowed only to the extent required for the purpose of the processing, and it must not encroach on the protection of privacy any more than is necessary. After processing, the location data must, unless otherwise provided by law, be destroyed or rendered such that it cannot be associated with a specific subscriber or user.
- (4) The prohibiting of the processing of location data and the service-specific consent referred to in this Chapter are decided in the case of minors under the age of 15 by their guardian under section 4 of the Child Custody and Right of Access Act (361/1983), and in the case of legally incompetent persons other than minors by their guardian under the Guardianship

Services Act (442/1999), unless this is impossible by virtue of the technical nature of the service.

Section 17 – Subscriber’s right to prohibit processing of location data

- (1) A telecommunications operator may process location data if the subscriber has not forbidden it.
- (2) The telecommunications operator must ensure that the subscriber can easily and at no separate charge prohibit processing of location data , unless otherwise provided by law.
- (3) The telecommunications operator must ensure that the subscriber has easy and continuous access to information on the precision of the location data processed, the purpose of the processing and whether location data can be disclosed to a third party for the purpose of providing value added services.
- (4) Before disclosing location data to a value added service provider or corporate or association subscriber, the telecommunications operator must take appropriate steps to ensure that the provision of such a value added service is based on the consent referred to in section 18(1).

Section 18 – Service-specific consent of the party to be located

- (1) The value added service provider or the corporate or association subscriber must request service-specific consent from the party to be located before beginning the processing of location data , unless such consent is unambiguously implied from the context or unless otherwise provided by law.

- (2) The party to be located must have the opportunity easily and at no separate charge to cancel the consent referred to in subsection 1, unless otherwise provided by law.
- (3) The value added service provider or corporate or association subscriber must ensure that the party to be located has easy and continuous access to information on the precision of the location data processed, on the exact purpose and duration of the processing and on whether the location data may be disclosed to a third party for the purpose of providing a value added service. The value added service provider or corporate or association subscriber must particularly ensure that this information is available to the party to be located before giving the consent referred to in subsection 1.

Chapter 5 – **Information security in communications**

Section 19 – *Obligation to maintain information security*

- (1) Telecommunications operators and value added service providers must maintain the information security of their services. Corporate or association subscribers must maintain information security in processing their users' identification data and location data . Maintaining information security in such services or processing means taking measures to ensure operating security, communications security, hardware and software security and data security. These measures must be commensurate with the seriousness of threats, level of technical development and costs.
- (2) Telecommunications operators and value added service providers are responsible to subscribers and users

for the information security referred to in subsection 1 also on the behalf of any third party that wholly or in part provides a network service, communications service or value added service. What is specified in this subsection applies to corporate or association subscribers with regard to the processing of users' identification data and location data .

- (3) The Finnish Communications Regulatory Authority may issue further regulations to a telecommunications operator regarding the information security of services referred to in subsections 1 and 2.

Section 20 – Measures taken to implement information security

- (1) In order to combat violations of information security and to remove information security disruptions, a telecommunications operator, value added service provider or corporate or association subscriber, or any party acting on their behalf has the right to undertake necessary measures in order to ensure information security as referred to in section 19:
 - 1) by preventing the transmitting and receiving of e-mail messages, text messages and other similar messages;
 - 2) by removing from the messages malicious software that endangers information security;
 - 3) by undertaking any other comparable technical measures.
- (2) The measures referred to in subsection 1 above may only be undertaken if they are necessary for the purpose of safeguarding network services, communications services or the communications ability of the recipient.

- (3) The content of any message may only be examined using technical means for inspection and removal if there is probable cause to suspect that such a message contains a computer program or section of code as referred to in Chapter 34, section 9a(1) of the Penal Code (39/1889), or if there is probable cause to suspect that the message is being used for disruption of telecommunications as referred to in Chapter 38, section 5 of the Penal Code.
- (4) Any measures undertaken must be implemented with care, and they must be commensurate with the seriousness of the disruption being combated. Such measures must not limit freedom of speech, the confidentiality of a message or the protection of privacy any more than is necessary for the purpose of safeguarding network services, communications services or the communications ability of the recipient. Such measures must be discontinued immediately when the conditions for them specified in this section no longer exist.
- (5) The Finnish Communications Regulatory Authority may issue further regulations on the technical measures for combating violations of information security and the removal of information security disruptions referred to in this section.

Section 21 – *Information security notifications*

- (1) If a specific threat applies to the information security of a service referred to in section 19, the telecommunications operator and value added service provider must immediately notify the subscriber of the threat and inform him or her of the measures available to subscribers and users for combating the threat, and the probable costs of such measures.

- (2) The telecommunications operator must notify the Finnish Communications Regulatory Authority of significant violations of information security in network services and communications services and of any information security threats to such services that come to the attention of the telecommunications operator. Furthermore, the telecommunications operator must notify the Finnish Communications Regulatory Authority of significant faults and disruptions in services. Notification must also be made of measures undertaken to prevent the reoccurrence of such violations of information security, threats of such violations, faults and disruptions.
- (3) Having combated a significant information security violation or threat concerning its service, or having removed a disruption, the telecommunications operator must publish an appropriate notification of the measures taken and any effects they may have on the use of that service.
- (4) The Finnish Communications Regulatory Authority may issue further regulations on the content, form and delivery to the Finnish Communications Regulatory Authority of the notifications referred to in subsections 1 and 2, or regulations on the content and form of the publication of information referred to in subsection 3.

Chapter 6 – **Telephone services**

Section 22 – *Subscriber connection identification*

- (1) A telecommunications operator offering a calling line identification service must offer subscribers an easy way of barring:

- 1) identification of any or all of his or her subscriber connections;
 - 2) identification of the subscriber connections of incoming calls;
 - 3) reception of calls whose subscriber connection identification is barred, if this is technically possible without undue cost; and
 - 4) identification of the subscriber connection to which incoming calls have been transferred.
- (2) The services referred to in paragraphs 1, 2 and 4 of subsection 1 must be free of charge to the subscriber.
- (3) A telecommunications operator offering a calling line identification service must offer the user an easy way of barring identification of his subscriber connection separately for each outgoing call, at no charge.
- (4) A telecommunications operator must notify subscribers and users of the services referred to in this section.
- (5) A telecommunications operator must ensure that the barring functions referred to in subsections 1 and 3 can be bypassed when disclosing data to emergency services authorities under section 35 or when complying with the right of the police to access information under section 36.
- (6) The Finnish Communications Regulatory Authority can issue technical regulations concerning the bypassing of the barring of subscriber connection identification referred to in subsections 1, 3 and 5.

Section 23 – *Automatic call transfer*

If a user so requests, a telecommunications operator must, at no charge, remove any automatic call transfer to the user's subscriber connection that has been placed by a third party.

Section 24 – *Call itemization of a bill*

- (1) A telecommunications operator may not release the call itemization of a bill, unless otherwise provided in this section.
- (2) In addition to the provisions on itemization in a telecommunications bill in section 80 of the Communications Market Act, a telecommunications operator must release the call itemization of a bill if the subscriber so requests. Such an itemization must be provided in a form where the last three digits of the phone number are obscured or the itemization otherwise rendered such that the other party of the communication cannot be identified.
- (3) A telecommunications operator must, if the user so requests, release the call itemization of a bill with the complete phone numbers or other communications service identification data of the parties to the communication. This right is exercised in the case of minors under the age of 15 by their guardian under section 4 of the Child Custody and Right of Access Act, and in the case of legally incompetent persons other than minors by their guardian under the Guardianship Services Act.
- (4) Notwithstanding the provisions of subsection 2, a telecommunications operator must release to the subscriber an itemization by service type for calls

for which the subscriber incurs charges beyond those related to the use of the communications service.

- (5) A call itemization for a subscriber connection may not contain identification data for services for which no fee is charged.
- (6) The Finnish Communications Regulatory Authority may issue further regulations on the content and implementation of the itemization referred to in this section.

Section 25 – Telephone directories, other subscriber directories and directory inquiries

- (1) A service provider providing a telephone directory, other subscriber directory or a directory inquiry service is entitled to process personal data for the purpose of creating and providing directory service or a directory inquiry service.
- (2) A subscriber's right to have his or her name, address and telephone number entered in a telephone directory is laid down in section 57 of the Communications Market Act. The obligation of a telecommunications operator or value added service provider to disclose contact information to other service providers for the purpose of preparing a telephone directory or providing a directory inquiry service is laid down in section 58 of the Communications Market Act.
- (3) A telecommunications operator must notify any subscriber who is a natural person about the purpose and use of any telephone directory or other subscriber directory that is publicly available or usable through a directory service, or any directory inquiry service. Such notification must be given at no charge before the subscriber's information is

entered in the subscriber directory or directory inquiry service.

- (4) A telecommunications operator must give any subscriber who is a natural person the opportunity to prohibit, at no charge, the inclusion of any part or all of his or her contact information in a telephone directory, other subscriber directory or directory inquiry service. The telecommunications operator and any company providing a subscriber directory service and directory inquiry service that has received such contact information under section 58 of the Communications Market Act must, if any subscriber who is a natural person so requests, remove and amend incorrect information at no charge. The right of access is laid down in section 26 of the Personal Data Act.
- (5) Any subscriber who is a natural person has the right to prohibit, at no charge, the disclosure of his or her contact information as referred to in this section to a third party.
- (6) A telecommunications operator must allow companies and other organizations entered in a telephone directory, other subscriber directory or directory inquiry service the right to have their contact information inspected and removed, and incorrect contact information amended.

Chapter 7 – **Direct marketing**

Section 26 – *Direct marketing to natural persons*

- (1) Direct marketing by means of automated calling systems, facsimile machines, or e-mail, text, voice,

sound or image messages may only be directed at natural persons who have given their prior consent.

- (2) Direct marketing other than referred to in subsection 1 to a natural person is allowed if the person has not specifically prohibited it. A natural person must be able easily and at no charge to prohibit direct marketing as referred to in this subsection.
- (3) Notwithstanding subsection 1, where a service provider or a product seller obtains from any customer who is a natural person his contact information for e-mail, text, voice, sound or image messages in the context of the sale of a product or service, that service provider or product seller may use this contact information for direct marketing of his or her own products of the same product group and of other similar products or services. The service provider or product seller must allow any customer who is a natural person the opportunity to prohibit, easily and at no charge, the use of contact information at the time when it is collected and in connection with any e-mail, text, voice, sound or image message. The service provider or product seller must notify the customer clearly of the possibility of such a prohibition.

Section 27 – Direct marketing to legal persons

- (1) Direct marketing to legal persons is allowed if the recipient has not specifically prohibited it.
- (2) Any legal person must be allowed the opportunity to prohibit, easily and at no separate charge, the use of its contact information in connection with any e-mail, SMS, voice, sound or image message sent in direct marketing. The party undertaking direct

marketing must give clear notification of the possibility of such a prohibition.

Section 28 – Identification of direct marketing

- (1) The recipient of an e-mail, text, voice, sound or image message sent for the purpose of direct marketing as referred to in sections 26 and 27 above must be able to recognize such a message as marketing clearly and unambiguously.
- (2) It is prohibited to send such an e-mail, text, voice, sound or image message intended for direct marketing that
 - 1) disguises or conceals the identity of the sender on whose behalf the communication is made; or
 - 2) is without a valid address to which the recipient may send a request that such communications be ended.

Section 29 – Preventing the reception of direct marketing

Telecommunications operators and corporate or association subscribers are entitled, at a user's request, to prevent the reception of direct marketing as referred to in sections 26-28. Such measures must be undertaken with care, and they must not restrict freedom of speech or encroach on the confidentiality of messages or the protection of privacy any more than is necessary.

Chapter 8 – **Guidance and supervision**

Section 30

General guidance and development

General guidance and development for the purpose of implementing this Act is the responsibility of the Ministry of Transport and Communications.

Section 31 – *Duties of the Finnish Communications Regulatory Authority*

The duties of the Finnish Communications Regulatory Authority are:

- 1) to supervise compliance with this Act and any provisions issued under it, unless otherwise provided in section 32;
- 2) to collect information on violations of and threats to information security in respect of network services, communications services and value added services, and on significant faults and disruptions in such services;
- 3) to investigate violations of and threats to information security in respect of network services, communications services and value added services, and significant faults and disruptions in such services; and
- 4) publicize information security matters.

Section 32 – *Duties of the Data Protection Ombudsman*

The duties of the Data Protection Ombudsman are to supervise:

- 1) the processing of location data referred to in Chapter 4 above;
- 2) compliance with the provisions on telephone directories and other subscriber directories, and

on directory inquiries, as referred to in section 25 above;

- 3) compliance with the provisions on direct marketing in Chapter 7 above; and
- 4) compliance with the provisions in Chapter 9 below on right of access and obligation of secrecy with respect to location data .

Chapter 9 – **Right of access to information**

Section 33 – *Guidance and supervision authorities' right of access to information*

- (1) Notwithstanding secrecy provisions and other restrictions on the disclosure of information, the Ministry of Transport and Communications, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman are entitled to access information necessary for the carrying out of their duties under this Act from any telecommunications operator, value added service provider, corporate or association subscriber, telecommunications contractor, service provider processing data describing the use of its service, direct marketing party, subscriber directory service or directory inquiry service provider, or anyone acting on their behalf, concerning their activities referred to in this Act. The right of access to information granted to the Ministry of Transport and Communications, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman does not apply to information on confidential messages, identification data or location data .
- (2) Notwithstanding the provisions of section 5, the Finnish Communications Regulatory Authority is entitled to access any identification data and

location data necessary for investigating a fault or disruption in a network service, communications service or value added service, or for clarifying anything in the billing.

- (3) The Finnish Communications Regulatory Authority and the Data Protection Ombudsman are entitled to access any identification data, location data and messages referred to in section 20(2) for carrying out their duties under this Act if they are required for supervision of compliance with the provisions on processing, the use of information referred to in section 7, or direct marketing, or for clarifying significant violations of or threats to information security, and if the Finnish Communications Regulatory Authority or the Data Protection Ombudsman have reason to believe that the essential elements of any of the following are present:
- 1) a breach of privacy protection in electronic communications under section 42(2) of this Act;
 - 2) unauthorized use under Chapter 28, section 7 of the Penal Code;
 - 3) endangering computerized data processing under Chapter 34, section 9a of the Penal Code;
 - 4) criminal damage under Chapter 35, section 1(2) of the Penal Code;
 - 5) a secrecy offence under Chapter 38, section 1 of the Penal Code;
 - 6) communications secrecy violation under Chapter 38, section 3 of the Penal Code;
 - 7) interference with communications under Chapter 38, section 5 of the Penal Code;
 - 8) unauthorised access to data under Chapter 38, section 8 of the Penal Code;
 - 9) an offence involving an illicit device for accessing protected services under Chapter 38, section 8a of the Penal Code;

- 10) a data protection offence under Chapter 38, section 9 of the Penal Code.
- (4) The Ministry of Transport and Communications, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman are only entitled to process the information they receive insofar as it is necessary to carry out their duties under this Act.
- (5) The Finnish Communications Regulatory Authority and the Data Protection Ombudsman must destroy any information on confidential messages, identification data and location data received under subsection 3 when this information is no longer necessary for carrying out the duties provided for in subsection 3 or the processing of any criminal case concerning the information. Information on confidential messages, identification data and location data must be destroyed no later than two years, or ten years in the case of information pertaining to an investigation of a violation of information security, from the end of the calendar year during which the information was received or a decision or sentence in the matters referred to in this subsection entered into legal force.
- (6) The right of access to information provided for in this section does not apply to the information referred to in section 94 of the Act on Credit Institutions (1607/1993) or in Chapter 17, section 24(2-3) of the Code of Judicial Procedure.

Section 34 – Supervision authorities' obligation of secrecy and disclosure of information

- (1) Any information on confidential messages, identification data and location data received by the Finnish Communications Regulatory Authority and

the Data Protection Ombudsman under section 33(3) must be kept secret.

- (2) Notwithstanding any restriction on the disclosure of information other than the secrecy provision of subsection 1, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman are entitled to disclose the information referred to in section 33(1) received in the course of carrying out their duties under this Act to the Ministry of Transport and Communications.
- (3) Notwithstanding the secrecy provision of subsection 1 or other restriction on the disclosure of information, the Finnish Communications Regulatory Authority is entitled to disclose identification data received in connection with collecting information on and investigating violations of information security to those telecommunications operators, value added service providers and corporate or association subscribers who have been abused in such a violation of information security or who have been the subject of such a violation of information security, if the Finnish Communications Regulatory Authority has reason to believe that the essential elements of any of the cases listed above in section 33(3)(1-10) are present.
- (4) The Finnish Communications Regulatory Authority is entitled to disclose the identification data referred to in subsection 3 only to the extent necessary to prevent and clarify violations of information security.
- (5) In all other cases, the secrecy of information held by the supervision authorities is governed by the Act on the Openness of Government Activities (621/1999).

Section 35 – *Disclosing information to emergency services authorities*

- (1) A telecommunications operator is obliged to disclose the following to an Emergency Response Centre, a Marine Rescue Coordination Centre, a Marine Rescue Sub-Centre or a Police Emergency Centre for processing purposes:
 - 1) identification data and location data of the subscriber connection and terminal device from which an emergency call is placed, and information on the subscriber, user and installation address; and
 - 2) identification data and location data showing the location of the user terminal device and subscriber connection to which the emergency call applies if, in the considered opinion of the authority receiving the emergency call, the user is in obvious distress or immediate danger.
- (2) The information referred to in subsection 1 above must be released notwithstanding the obligation of secrecy referred to in section 5 and the requirements for processing location data specified in Chapter 4, and without reference to what the subscriber or user may have agreed with the telecommunications operator concerning the secrecy of such information.
- (3) A value added service provider is entitled to disclose the information referred to in subsection 1 to an Emergency Response Centre, a Marine Rescue Coordination Centre, a Marine Rescue Sub-Centre or a Police Emergency Centre.
- (4) A telecommunications operator must immediately notify an Emergency Response Centre, Marine Rescue Coordination Centre, Marine Rescue Sub-Centre and Police Emergency Centre of any disruptions in

communications networks, network services and communications services which are significant for the transmission of emergency calls.

- (5) Compensation for costs incurred in fulfilling the obligations provided for in subsection 1 above is provided for in section 98 of the Communications Market Act.

Section 36 – Certain other authorities' right of access to information

- (1) The right of authorities to receive identification data for the purpose of preventing and uncovering crimes is laid down in the Police Act (493/1995) and the Customs Act (1466/1994). The right of authorities to receive identification data for the purpose of investigating a crime is laid down in the Coercive Measures Act (450/1987).
- (2) Notwithstanding the obligation of secrecy provided in section 5, the police are entitled to receive from a telecommunications operator:
 - 1) identification data on transmissions to a particular subscriber connection, with the consent of the injured party and the possessor of the subscriber connection, necessary for the purpose of investigating a violation of a restraining order under Chapter 16, section 9a of the Penal Code, criminal disturbance under Chapter 17, section (13)(2) of the Penal Code or breach of domestic peace under Chapter 24, section 1(2) of the Penal Code; and
 - 2) identification data on messages transmitted from a particular mobile communications device, with the consent of the subscriber or owner of the device, insofar as necessary for investigating a crime where the mobile communications device or the

subscriber connection used therein has been unlawfully in the possession of another party.

- (3) Provisions on compensation for costs incurred by fulfilling the obligations provided above in this section are laid down in section 98 of the Communications Market Act.

Section 37 – *User’s special right of access to information*

- (1) A user is entitled to receive from a telecommunications operator the identification data possessed by the latter showing the location of the subscriber connection or terminal device at a given moment.
- (2) The right referred to in subsection 1 above is exercised in the case of minors under the age of 15 by their guardian under section 4 of the Child Custody and Right of Access Act and in the case of legally incompetent persons other than minors by their guardian under the Guardianship Services Act.

Chapter 10 – **Information security fee**

Section 38 – *Determination of the fee*

A telecommunications operator subject to notification or licence shall pay an annual information security fee to the Finnish Communications Regulatory Authority. The information security fee covers the costs incurred by the Finnish Communications Regulatory Authority for carrying out the duties provided in this Act concerning telecommunications operators.

Section 39 – *Amount of the information security fee*

- (1) No information security fee is charged on the turnover from television and radio broadcasting activities as referred to in the Act on Television and Radio Operations (744/1998) or on the relaying of television or radio broadcasts.
- (2) The information security fee is determined in payment units according to payment categories. One payment unit equals EUR 80. Operators are assigned to payment categories in order to take into account the average costs incurred by the Finnish Communications Regulatory Authority for carrying out the duties related to operators in the respective category. The payment category for each operator is determined by the turnover that the operator has for telecommunications activities in Finland during the period that precedes the determination of the fee.
- (3) If a telecommunications operator is part of a corporate group as referred to in Chapter 1(6) of the Accounting Act (1336/1997), the basis for the telecommunications operator's fee is the operator's share of the total turnover from telecommunications activities in Finland of the group's liable operators less their intra-company turnover from these activities. For the fee to be levied, it is further required that an operator being part of a group of companies has telecommunications turnover subject to the information security fee. If the parent company is not Finnish, the basis for the fee remains the same.
- (4) Further provisions on how the information necessary for determining the fee is to be notified to the Finnish Communications Regulatory Authority may be

issued by decree of the Ministry of Transport and Communications.

The information security fee is determined as follows:

Payment category	Turnover (EUR million)	Number of units
1	less than 1	2
2	1 – less than 2	4
3	2 – less than 4	7
4	4 – less than 8	14
5	8 – less than 16	26
6	16 – less than 32	50
7	32 – less than 64	94
8	64 – less than 128	179
9	128 – less than 256	340
10	256 – less than 512	645
11	512 – less than 1,024	1,226
12	more than 1,024	2,330

Section 40 – Stipulating and collecting the information security fee

- (1) The obligation for an operator to pay an information security fee is stipulated by the Finnish Communications Regulatory Authority. Further provisions on the collecting of the fee may be given by decree of the Ministry of Transport and Communications.
- (2) An information security fee may be collected without a judgment or decision under the Act on the Recovery of Taxes and Fees by Recovery Proceedings (367/1961). If the fee is not settled by the due date, annual penalty interest on delayed payments will be charged

for the unpaid amount according to the interest rate referred to in section 4 of the Interest Act (633/1982). Instead of the penalty interest, the authority may collect a default payment of EUR 5 if the amount of the penalty interest is less than that.

Chapter 11 – **Miscellaneous provisions**

Section 41 – *Coercive measures*

- (1) If someone violates this Act or provisions issued under it and, despite being requested to do so, fails to rectify his actions within a specified reasonable period, the Finnish Communications Regulatory Authority, in carrying out the duties specified in section 31(1), or the Data Protection Ombudsman, in carrying out the duties specified in section 32, may order him or her to rectify the error or omission. The Finnish Communications Regulatory Authority or the Data Protection Ombudsman may impose a conditional fine or a threat of having the act done at the defaulter's expense as sanctions in support of the obligation. If the violation is severe, such a threat may also involve terminating the violator's business in part or in full.
- (2) The Finnish Communications Regulatory Authority and the Data Protection Ombudsman may submit any matter processed by them to pre-trial investigation.
- (3) The provisions on conditional fines, threat of termination and threat of completion laid down in the Act on Conditionally Imposed Fines (1113/1990) apply. The costs of action taken at the defaulter's expense are paid provisionally from government funds. These costs may be collected without a judgment or a

decision under the Act on the Recovery of Taxes and Fees by Recovery Proceedings.

Section 42 – *Penal provisions*

- (1) The penalties for communications secrecy violation and aggravated communications secrecy violation are provided in Chapter 38, sections 3 and 4 of the Penal Code, and the penalty for unauthorised access to data in Chapter 38, section 8 of the Penal Code. The penalty for a breach of the obligation of secrecy provided in section 5 is subject to Chapter 38, section 1 or 2 of the Penal Code, unless the offence is punishable under Chapter 40, section 5 of the Penal Code or unless a more severe penalty is provided elsewhere.
- (2) Whoever wilfully
 - 1) violates the prohibition on the possession, importing, manufacture and distribution of any system or part thereof for decoding the technical protection of electronic communications provided in section 6(2);
 - 2) neglects the duties provided in section 7;
 - 3) neglects the duties provided in section 19 regarding the information security of his or her services or of the processing of identification data and location data ;
 - 4) neglects the notification requirement provided for in section 21(2) or section 35(4);
 - 5) processes identification data or location data in violation of what is provided in Chapters 3 and 4;
 - 6) neglects to comply with the provisions of section 24 regarding call itemization of bills;
 - 7) neglects to comply with the provisions of section 25 regarding the processing of personal data contained in telephone directories and other

subscriber directories, the notifying of subscribers regarding the purpose and use of such directories, the removing and rectifying of information, the right to prohibit use or the rights of legal persons; or

- 8) practices direct marketing in violation of provisions in Chapter 7, shall be imposed a fine for a *violation of protection of privacy in electronic communications*, unless a more severe penalty is provided elsewhere.

- (3) If the offence is deemed petty, sentence shall not be passed.

Section 43 – *Appeal*

An appeal may be made in compliance with the provisions of the Administrative Judicial Procedure Act (586/1996) against decisions of the Finnish Communications Regulatory Authority or the Data Protection Ombudsman taken under this Act. In their decisions, the Finnish Communications Regulatory Authority and the Data Protection Ombudsman may order that the decision be complied with before it has gained legal force. However, the appellate authority may prohibit enforcement until the appeal has been resolved.

Section 44 – **Transitional provisions and entry into force**

- (1) This Act enters into force on 1 September 2004.
- (2) This Act repeals:
- 1) the Act on the Protection of Privacy and Data Security in Telecommunications of 22 April 1999 (565/1999) as amended; and
 - 2) sections 3(6) and 18 of the Decree of the Ministry of Transport and Communications on the Fees of

the Finnish Telecommunications Regulatory
Authority of 11 December 2002 (1126/2002).

- (3) Measures necessary for the implementation of this Act may be undertaken before the Act's entry into force.
- (4) If a telecommunications operator has begun the processing of location data under then current regulations before this Act's entry into force, subscribers must be notified of the processing of location data within six months of the Act's entry into force. If a subscriber does not prohibit processing of such data within three months of such notification, the processing of such location data may be continued subject to the provisions of Chapter 4.
- (5) A telecommunications operator must begin the saving of data referred to in section 15 within six months of this Act's entry into force.
- (6) Provisions of section 25 above do not apply to subscriber directory editions that were already produced or distributed in printed form or any other form except online electronic form before this Act's entry into force. If a subscriber's or user's information is entered into a subscriber directory in online electronic form compliant with the provisions of the Act on the Protection of Privacy and Data Security in Telecommunications before this Act's entry into force, the telecommunications operator and the subscriber directory and directory inquiry service provider who has received the contact information under section 58 of the Communications Market Act must provide any subscriber who is a natural person with information on the purpose or use of the subscriber directory and the subscriber's rights under section 25(4-5) within one year of this

Act's entry into force. If such a subscriber who is a natural person does not request that his or her contact information be removed, that information may be retained in the subscriber directory.

- - -

This Act enters into force on 1 September 2004.