NB: Unofficial translation;
legally binding only in Finnish and Swedish

Act on the Protection of Privacy in Electronic Communications

(516/2004; amendments up to 365/2011 included)

Chapter 1 - *General provisions*

Section 1 - *Objectives*

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; (198/2006)

14) *processing* means collecting, saving, organizing, using, transferring, disclosing, storing, modifying, combining, protecting, removing, destroying and other similar actions; (198/2006)

14 a) *service operator* means an operator referred to in section 2(19) of the Communications Market Act; (343/2008)

14 b) *Internet phone service* means service provided by telecommunications operators enabling calls that are based on Internet protocol through to the end customer; (343/2008)

15) *targeted emergency message* means a message to prevent an imminent threat to human lives, health, property or an imminent threat of considerable damage to property or the environment that will be communicated in mobile network by means of an SMS, for example, to terminals or subscriber connections within a certain area or areas; (198/2006)

16) *other targeted message from the authorities* means a message to protect people and property that will be communicated in mobile network by means of an SMS, for example, to terminals or subscriber connections within a certain area or areas when the threat to human lives, health or property is not imminent; (198/2006)

17) *targeted message from the authorities* means a targeted message in the event of an emergency and any other targeted message from the authorities; (1328/2007)

18) *telecommunications contractor* means a natural or legal person that for the purposes of practising a livelihood constructs, installs or maintains an internal communications network in a property or building that is intended for connection to a public communications network. (1328/2007)

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) If not 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.

(9) Act on the Protection of Privacy in Working Life (477/2001) has been repealed by the Act of 13 August 2004 (759/2004). Act on Preventing and Clearing Money Laundering (68/1998) has been repealed by the Act of 18 February 2008 on Preventing and Clearing Money Laundering and Financing of Terrorism (503/2008).

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) When a message has been transmitted to be universally received, it is not confidential. The identification data associated with such a message is, however, confidential. Provisions on disclosing 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 shall 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 shall 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 shall not disclose knowledge obtained through their employment about messages, identification data or 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. (1328/2007)

(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 of a system for decoding the technical protection of electronic communications is prohibited in cases where such a system or part of a system 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 (365/2011) - *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 save cookies or other data concerning the use of the service in the user's terminal device, and use such data, if the user has given his or her consent thereto and the service provider gives the user comprehensible and complete information on the purposes of saving or using such data.

(2) Provisions of subsection 1 above do not apply to any saving or use of data which is intended solely for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider 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 limit the protection or privacy any more than is necessary.

Chapter 3 - *Processing 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 below is only allowed to the extent necessary for the purpose of such processing, and it may not limit 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. (343/2008)

Section 9 (125/2009) - *Processing identification data for the purpose of providing and using services*

(1) Identification data may only be processed to the extent necessary for providing and using a network service, communications service or value added service and for the purpose of ensuring information security as provided below.

(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, corporate or association subscriber, or a subscribing legal person for the purpose of processing data to perform the functions referred to separately in this Chapter.

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 (125/2009) - *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 network services, communications services or value-added services.

(2) A corporate or association subscriber may process identification data for the purpose of technical development of its own communications network and own services connected to it.

(3) Prior to the start of the processing referred to in subsection 1, subscribers or users shall be informed of what identification data is to be processed and how long the processing will last. The information may be given only once.

Section 12 a (125/2009) - *Processing for the purposes of statistical analysis*

(1) For the purposes of statistical analysis, automatic data processing may be used by a telecommunications operator or a value-added service provider for processing identification data, and by a corporate or association subscriber for processing identification data of its communications network or a connected service, if:

1) the analysis cannot be made by any other means without undue difficulty; and

2) no individual natural person can be identified in the analysis.

(2) Provisions of section 1 shall also apply to a subscribing legal person's right to process the identification data related to its subscription and terminal device.

Section 13 (125/2009) - *A telecommunications operator's and value added service provider's right to process data in cases of misuse*

(1) A telecommunications operator and a value added service provider may process identification data for detecting, preventing or investigating any non-paying use of fee-based network services, communications services or value added services, or any similar cases of misuse.

(2) The Finnish Communications Regulatory Authority may issue further regulations on the technical implementation of the processing of identification data referred to in subsection 1.

Section 13a (125/2009) - *A corporate or association subscriber's right to process data in cases of misuse*

(1) A corporate or association subscriber has the right to process identification data to prevent or investigate unauthorised use of information society service or of communications network or service, or to prevent and investigate the disclosure of business secrets referred to in Chapter 30(11) of the Penal Code (39/1889) as provided in sections 13b-13k of this Act.

(2) Unauthorised use of a communications network or service may be considered to be installation of a device, software or service in the communications network of a corporate or association subscriber, providing unlawfully a third party with access to the communications network or service of a corporate or association subscriber, or any other comparable use of a communications network or service if it contradicts with the instructions provided in section 13b(3).

(3) The right referred to above in subsection 1 does not apply to the identification data of telephone services in a fixed or mobile network.

Section 13b (125/2009) - *A corporate or association subscriber's duty of care in cases of misuse*

(1) Before starting to process identification data and in order to prevent unauthorised use of information society service or communications network or service liable to charge, a corporate or association subscriber shall:

1) restrict access to its communications network and service and to their use and take other steps in order to protect the use of its communications network and service with the help of appropriate information security measures;

2) define the type of messages that may be transmitted and searched through its communications network and how its communications network and service may be used and the addresses to which no messages may be communicated.

(2) In order to prevent business secrets from being disclosed, a corporate or association subscriber shall, before starting to process identification data:

1) restrict access to business secrets and take other steps in order to protect the use and data of its communications network and service with the help of appropriate information security measures;

2) define how business secrets may be transferred, delivered or otherwise handled in a communications network and define the type of addresses to which messages may not be sent by people entitled to handle business secrets.

(3) A corporate or association subscriber shall provide the users of a communications network or service with written instructions on preventing misuse referred to in subsections 1 and 2.

Section 13c (125/2009) - *A corporate or association subscriber's duty of planning and cooperation in cases of misuse*

(1) A corporate or association subscriber shall, before starting to process identification data referred to in section 13a(1), name the people whose duties involve identification data processing or define the duties involved.

Identification data may only be processed by people responsible for maintenance and information security of a corporate or association subscriber's communications network or service and by people responsible for security.

(2) If the corporate or association subscriber is an employer that falls within the scope of cooperation legislation, it shall:

1) discuss the reasons and procedures to be followed in identification data processing referred to in sections 13a-13k in a cooperation procedure referred to in Chapter 4 of the Act on Cooperation within Undertakings (334/2007), in the Act on cooperation within government agencies (651/1988), and in the Act on cooperation between the employer and employees in municipalities (449/2007);

2) inform employees or their representatives the decisions taken regarding identification data processing as provided in section 21(2) of the Act on the Protection of Privacy in Working Life (759/2004).

(3) If the corporate or association subscriber is an employer that does not fall within the scope of cooperation legislation, it shall hear the employees about issues referred to in subsection 2(1) of this section and inform the employees about them as provided in section 21(1 and 2) of the Act on the Protection of Privacy in Working Life.

(4) If the corporate or association subscriber is not the employer, it shall inform the users of the procedures to be followed in identification data processing referred to in sections 13a-13k.

Section 13d (125/2009) - *A corporate or association subscriber's right to process data for investigating unauthorised use of information society service, communications network or communications service*

(1) A corporate or association subscriber may process identification data with the help of an automatic search function that may be based on the size, aggregate size, type, number, connection mode or target addresses of the messages.

(2) A corporate or association subscriber may process identification data manually, if there are reasonable grounds to suspect that a communications network, communications service or an information society service subject to a fee is used against the instructions referred to in section 13b(3) and if:

1) a deviation in communications has been detected in the automatic search;

2) the costs of using an information society service subject to a fee have risen to an unusually high level;

3) a communications network is detected to use an unlawfully installed device, software or service; or

4) in an individual case, some identifiable circumstance comparable to subsections 1-3 leads to the conclusion that a communications network, communications service or an information society service subject to a fee is used against the instructions referred to in section 13b(3).

(3) A requirement for the processing referred to in sections 1 and 2 above is that the event or act would probably cause significant hindrance or damage to the corporate or association subscriber.

(4) A further requirement for the processing referred to in section 2 above is that the data is necessary for investigating the unauthorised use and the parties responsible for it and for ending the unauthorised use.

Section 13e (125/2009) - *A corporate or association subscriber's right to process data for investigating disclosures of business secrets*

(1) A corporate or association subscriber may process identification data with the help of an automatic search function that may be based on the size, aggregate size, type, number, connection mode or target addresses of the messages.

(2) A corporate or association subscriber may process identification data manually, if there are reasonable grounds to suspect that a business secret has been disclosed to a third party without permission via a communications network or communications service:

1) a deviation in communications has been detected in the automatic search;

2) a business secret is published or used without permission, or

3) in an individual case, some identifiable circumstance comparable to subsections 1 or 2 leads to the conclusion that access to a business secret has been disclosed to a third party without permission.

(3) The requirement for the processing referred to in sections 1 and 2 above is that the business secrets suspected to have been disclosed are of major significance to the corporate or association subscriber's or its cooperation partner's business or to the results of technological or other development work likely to be important for establishing or practising a livelihood.

(4) A further requirement for the processing referred to in section 2 above is that the data is necessary for investigating the disclosure of the business secret and the parties responsible for it.

Section 13f (125/2009) - *Special restrictions to the right to process data in cases of misuse*

(1) An automatic search shall not be targeted and identification data shall not be searched or manually processed for finding out data referred to in Chapter 17(24)(2 and3) of the Code of Judicial Procedure.

(2) In order to investigate business secrets, a corporate or association subscriber that is an employer may only process the identification data of users to whom the corporate or association subscriber has provided access to business secrets or of users who through some other means accepted by the corporate or association subscriber have access to business secrets.

Section 13g (125/2009) - *A corporate or association subscriber's obligation to inform the user in cases of misuse*

(1) A corporate or association subscriber shall draw up a report of manual processing of identification data referred to in section 13d(2) and 13e(2) showing:

1) the grounds for the processing, and the time and duration of the processing:

2) the reason for using manual processing of identification data;

3) names of the processors involved;

4) name of the person who has made the processing decision.

(2) People involved in the processing shall sign the report. The report shall be kept for at least two years from the end of the processing referred to in sections 13d or 13e.

(3) A report referred to in section 1 above shall be delivered to the user of the communications network or service involved as soon as it is possible without endangering the purpose of the processing itself. No report needs to be delivered, however, to users whose identification data have been processed as mass data so that the identification data have not been known by the processor. Notwithstanding confidentiality requirements, the user has the right to submit the report and the related data for the purpose of managing matters related to the user's interests or rights.

Section 13h (125/2009) - *A corporate or association subscriber's obligation to inform the employees' representative in cases of misuse*

(1) If the corporate or association subscriber is an employer, it shall draw up an annual report to the employees' representative of manual processing of identification data referred to in section 13d(2) and 13e(2) showing the grounds for and the number of times of identification data processing during the year.

(2) A report referred to in section 1 above shall be delivered to a local union representative elected under a collective agreement or a collective agreement for civil servants, or, if no local union representative has been elected, to elected representatives referred to in Chapter 13(3) of the Employment Contracts Act (55/2001). If the employees of a personnel group have not elected a representative or a local union representative, the report shall be delivered to a cooperation representative referred to in section 8 of the Act on Cooperation within Undertakings, or to a cooperation representative referred to

in section 3 of the Act on cooperation between the employer and employees in municipalities, or to a representative referred to in section 6(2) of the Act on cooperation within government agencies. If these have not been elected either, the report shall be delivered to all employees of the personnel group in question.

(3) Employee representatives and employees referred to in section 2 shall treat any business secret infringements and suspected business secret infringements brought to their attention as confidential throughout their employment relationship. The provisions laid down in the Act on the Openness of Government Activities (621/1999) and elsewhere in law shall apply to secrecy obligation of public servants. Notwithstanding the provisions above, information may be disclosed to the supervision authorities.

Section 13i (125/2009) - *Prior notification and annual report to the Data Protection Ombudsman in cases of misuse*

(1) A corporate or association subscriber shall inform the Data Protection Ombudsman in advance of processing identification data. A prior notification shall explain:

1) the grounds and procedures for the measures to be followed in processing identification data referred to in sections 13d and 13e;

2) the duties referred to in section 13c(1);

3) the way in which the corporate or association subscriber has met its obligation to provide information before the processing referred to in section 13c(2)(2) or 13c(3).

(2) A corporate or association subscriber shall annually inform the Data Protection Ombudsman of manual processing of identification data after the processing has taken place. The report shall reveal the grounds for and the number of times of identification data processing during the year.

Section 13j (125/2009) - *A corporate or association subscriber's right to store identification data in cases of misuse*

Provisions of sections 13a-13i do not provide a corporate or association subscriber the right to store identification data in its registers longer than laid down in law.

Section 13k (125/2009) - *A corporate or association subscriber's right to forward data in cases of misuse*

Notwithstanding the provisions of section 8(3), a corporate or association subscriber has the right, in connection with a report of an offence or a request for an investigation it has filed as an injured party, to forward to the police for investigation identification data regarding messages of a user of a corporate or association subscriber's communications network or service that has been received in accordance with sections 13a-13j.

Section 14 (125/2009) - *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, preventing or investigating a technical fault or error in the transmission of communications.

Section 14a (343/2008) - *Obligation to store data for the purposes of the authorities*

(1) Notwithstanding the provisions of this Chapter concerning the processing of identification data, a service operator obliged to submit a telecommunications notification shall ensure, under the conditions prescribed below, that data referred to in Article 5 of the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC are retained for a period of 12 months from the date of the communication. Such data may be used only for the purposes of investigating, solving and considering charges for criminal acts referred to in Chapter 5 a(3)(1) of the Coercive Measures Act (450/1987).

(2) The retention obligation applies to data related to:

1) a service operator’s telephone service or additional service through a fixed network, telephone service, additional service, SMS service, EMS service or multimedia service through a mobile network;

2) Internet connection service provided by a service operator;

3) e-mail service provided by a service operator;

4) Internet telephony service provided by a service operator;

5) a call for which a connection has been established but the call remains unanswered or is prevented from being connected due to network management measures.

(3) The retention obligation does not apply to the contents of a message or identification data generated through the browsing of websites.

(4) A requirement for the retention obligation is that the data is available and generated or processed in connection with publicly available communications services provided on the basis of this Chapter or the provisions of the Personal Data Act.

(5) Further provisions on a more specific definition of data under the retention obligation may be issued by Government decree.

(6) Technical details of data under the retention obligation are defined in a Finnish Communications Regulatory Authority regulation.

Section 14b (343/2008) - *Obligations and procedures for processing data retained for the purposes of the authorities*

(1) A service operator under the retention obligation shall discuss the implementation and application of data retention with the Ministry of the Interior in order to ensure that all data considered necessary by the authorities will be retained. If no consensus is reached on the implementation of data retention,

the service operator decides on the technical implementation of the retention. The implementation shall follow the principles of cost-efficiency and consider the business needs of the service operator, the technical features of the systems, and the needs of the authority paying for the costs for the retention. Data should be retained in such a way as to avoid the same data being retained by several service operators. It must be ensured that the data retained can be transmitted to the authorities entitled to it without undue delay. A service operator under the retention obligation shall, together with a network operator if necessary, ensure that the obligation is met in such a way that the available data referred to in section 14 a processed by the network operator in providing the service operator's service shall be retained. A service operator under the retention obligation shall ensure that information about data retention and its purposes is available to the subscriber.

(2) Provisions on compensation for costs incurred by fulfilling the retention obligation and preparing for it are laid down in section 98 of the Communications Market Act. Provisions on retaining data for the purpose of investigating a single crime are laid down in Chapter 4(4 b and c) of the Coercive Measures Act.

(3) Further provisions on meeting the retention obligation may be given by Government decree.

(4) The Finnish Communications Regulatory Authority may issue further orders on the technical implementation of the retention obligations.

Section 14 c (343/2008) - *Statistics concerning the use of data to be retained for the purposes of the authorities*

(1) The Ministry of the Interior shall provide the Commission of the European Communities on a yearly basis with statistics on using data retained by virtue of this Act. The statistics shall include:

1) the cases in which retained data was provided to the authorities;

2) the cases where the authorities' requests for retained data could not be met;

3) the time elapsed between the date on which the data were retained and the date on which the authorities requested for the data.

(2) The Ministry of the Interior shall in particular take the statistics referred to above in subsection 1 into account in its reports about telecommunications interception and monitoring to Parliamentary Ombudsman by virtue of the Police Act (493/1995), Coercive Measures Act or any other Act.

Section 15 - *Saving information on processing*

(1) A telecommunications provider shall 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 shall 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 shall 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 shall not limit the protection of privacy any more than is necessary. After processing, the location data shall, 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall 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 shall maintain the information security of their services. Corporate or association subscribers shall 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 shall be commensurate with the seriousness of threats, level of technical development and costs.

(2) The obligation to maintain information security of services laid down in subsection 1 above also applies to processing of data for the purpose of meeting the retention obligation referred to in section 14 a. A service operator shall also name the people entitled to process retained data. (343/2008)

(3) Telecommunications operators and value added service providers are responsible to subscribers and users for the information security referred to in subsections 1 and 2 also on the behalf of any third party that wholly or in part provides a network service, communications service, data retention or value

added service. The responsibility specified in this subsection applies to corporate or association subscribers with regard to the processing of users' identification data and location data processed by a third party. (343/2008)

(4) The Finnish Communications Regulatory Authority may issue further regulations to a telecommunications operator regarding information security of services or of data retention referred to in subsections 1–3. (343/2008)

Section 20 (125/2009) - *Measures taken to implement information security*

(1) 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 referred to in section 2 for ensuring information security:

1) in order to detect, prevent, investigate and commit to pre-trial investigation any disruptions in information security of communications networks or related services;

2) in order to safeguard the communications ability of the sender or the recipient of the message; or

3) in order to prevent preparations of means of payment fraud referred to in Chapter 37(11) of the Penal Code planned to be implemented on a wide scale via communication services.

(2) Measures referred to in subsection 1 above may include:

1) automatic analysis of message content;

2) automatic prevention or limitation of message conveyance or reception;

3) automatic removal from messages of malicious software that pose a threat to information security;

4) any other comparable technical measures.

(3) If it is evident due to the message type, form or some other similar reason that the message contains a malicious software or command, and automatic content analysis of the message cannot ensure the attainment of the goals referred to in subsection 1, the contents of a single message may be processed manually. The sender and recipient of a message whose contents have been manually processed shall be informed of the processing, unless the information would apparently endanger the attainment of the goals referred to in subsection 1.

(4) Any measures referred to in this section shall be implemented with care, and they shall be commensurate with the seriousness of the disruption being combated. Such measures shall 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 the goals referred to in subsection 1. Such measures shall be discontinued if the conditions for them specified in this section no longer exist.

(5) The Finnish Communications Regulatory Authority may issue further regulations to telecommunications operators and value added service providers on the technical implementation of the measures referred to in this section.

Section 21 (365/2011) - *Information security notifications to the Finnish Communications Regulatory Authority*

(1) The telecommunications operator must notify the Finnish Communications Regulatory Authority without undue delay 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. A notification shall also be made of consequences of information security violations and of measures undertaken to prevent the reoccurrence of such violations and threats of such violations.

(2) If according to the Finnish Communications Regulatory Authority the notification of information security violation referred to in subsection 1 is in the public interest, it may order the telecommunications operator to provide information regarding the matter.

(3) The Finnish Communications Regulatory Authority may issue further regulations on the content, form, and delivery to the Finnish Communications Regulatory Authority of the notification referred to in subsection 1.

Section 21 a (365/2011) - *Information security notifications to subscribers and users*

(1) If a specific violation or threat is posed to the information security of a service referred to in section 19, the telecommunications operator and value added service provider shall immediately notify the subscriber and the user and inform them of the measures available to them for combating the threat, of the probable costs of such measures, and inform the sources of further information available to them.

(2) The telecommunications operator and value added service provider shall retain the data regarding the notifications.

(3) Having combated a significant information security violation or threat concerning its service, 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 and form of the notifications referred to subsection 1 and of the publication of information referred to in subsection 3, and on the retaining of notifications referred to in subsection 2. The Finnish Communications Regulatory Authority may also issue regulations on how it shall be informed of the notifications referred to in subsections 1 and 2 and of the publication of information referred to in subsection 3.

Section 21b (365/2011) – *Security audit*

(1) The Finnish Communications Regulatory Authority has the right to carry out a security audit of a telecommunications operator in order to supervise compliance with the obligations imposed in this Chapter.

(2) The Finnish Communications Regulatory Authority has the right to commission security audit measures to an independent expert. Provisions regarding criminal liability as a public official shall be applied to the expert while the

expert is performing duties under this section. Provisions of the Tort Liability Act (412/1974) shall apply to liability for damages.

(3) In the security audit, the Finnish Communications Regulatory Authority or any party acting on its behalf has the right to access the telecommunications operator's equipment facilities and other premises and to obtain for examination documents that are necessary for its supervision duty.

(4) No security audit shall be performed in premises used for residence of a permanent nature covered by the provisions on domestic peace.

(5) The costs of the security audit shall be covered by information security fee referred to in Chapter 10.

Chapter 6 - *Telephone services*

Section 22 - *Subscriber connection identification*

(1) A telecommunications operator offering a calling line identification service shall 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 shall notify subscribers and users of the services referred to in this section.

(5) A telecommunications operator shall 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 may 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 shall, 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 shall release the call itemization of a bill if the subscriber so requests. Such an itemization shall 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 shall, 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 shall 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 must 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 shall 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 shall be given at no charge before the subscriber's information is entered in the subscriber directory or directory inquiry service.

(4) A telecommunications operator shall 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 shall, 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 shall 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 that 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 shall 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 shall 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 shall 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 shall 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 shall 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;

2) is without a valid address to which the recipient may send a request that such communications be ended;

3) solicits recipients to visit websites that contravene Chapter 2 of the Consumer Protection Act (38/1978). (365/2011)

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 limit 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*

(1) The Finnish Communications Regulatory Authority shall

1) supervise compliance with this Act and any provisions issued under it, unless otherwise provided in section 32;

2) collect information on violations of and threats to information security in respect of network services, communications services and value added services;

3) investigate violations of and threats to information security in respect of network services, communications services and value added services;

4) publicize information security matters;

5) provide the European Commission and the European Network and Information Security Agency with an annual summary report of notifications referred to in section 21;

6) notify the European Commission of such cooperation with a European Union Member State which results in the harmonisation of control measures pertaining to the information security of communications services provided across the borders of Member States which may have an effect on the functioning of the internal market. (365/2011)

(2) In drafting regulations by virtue of this Act, the Finnish Communications Regulatory Authority shall consult the Ministry of Transport and Communications and work in cooperation with it. (343/2008)

Section 32 (125/2009) - *Duties of the Data Protection Ombudsman*

(1) The Data Protection Ombudsman shall supervise:

1) corporate or association subscribers' processing of identification data referred to in sections 13a–13k;

2) the processing of location data referred to in Chapter 4;

3) compliance with the provisions on telephone directories and other subscriber directories, and on directory inquiries, as referred to in section 25;

4) compliance with the provisions on direct marketing in Chapter 7;

5) compliance with the provisions in Chapter 9 on right of access and obligation of secrecy with respect to location data.

(2) A charge for performing the supervision duties referred to in section 1(1) above may be levied from corporate or association subscribers. A decision on measures subject to a charge and on the amount of the charge is to be taken in accordance with the criteria provided in the Act on Criteria for Charges Payable to the State (150/1992).

Chapter 9 - *Right of access to information, and a targeted message from the authorities* (198/2006)

Section 33 - *Guidance and supervision authorities' right to access information* (125/2009)

(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 or messages for the carrying out of their duties under this Act, if the data is required for supervising the 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. A further requirement is that the Finnish Communications Regulatory Authority or the Data Protection Ombudsman has reason to believe that the essential elements of any of the following are present: (125/2009)

1) a breach of privacy protection in electronic communications under section 42(2) of this Act;

2) unauthorized use under Chapter 28(7) of the Penal Code;

3) endangering computerized data processing under Chapter 34(9a) of the Penal Code;

4) criminal damage under Chapter 35(1)(2) of the Penal Code;

5) a secrecy offence under Chapter 38(1) of the Penal Code;

6) communications secrecy violation under Chapter 38(3) of the Penal Code;

7) interference with communications under Chapter 38(5) of the Penal Code;

8) unauthorised access to data under Chapter 38(8) of the Penal Code;

9) an offence involving an illicit device for accessing protected services under Chapter 38(8a) of the Penal Code;

10) a data protection offence under Chapter 38(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 shall 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 shall 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 141 of the Act on Credit Institutions (121/2007) or in Chapter 17(24)(2-3) of the Code of Judicial Procedure. (144/2007)

Section 34 (125/2009) - *Supervision authorities' obligation of secrecy*

(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) and any information received by the Data Protection Ombudsman under section 13i shall be kept secret.

(2) Other provisions on the secrecy of information held by the supervision authorities are issued in the Act on the Openness of Government Activities.

Section 34 a (125/2009) - *Disclosure of information held by the supervision authorities*

(1) Notwithstanding any restriction on the disclosure of information other than the secrecy obligation provided in section 34(1), the Finnish Communications Regulatory Authority and the Data Protection Ombudsman are entitled to disclose 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.

(2) Notwithstanding the secrecy provision of section 34(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 are likely to become 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.

(3) Notwithstanding the secrecy provision of section 34(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 or investigating violations of information security to competent authorities or other bodies that operate in another state preventing or investigating information security violations in communications networks and services.

(4) The Finnish Communications Regulatory Authority is entitled to disclose the identification data referred to in subsections 2 and 3 only to the extent necessary to prevent and investigate violations of information security. The disclosure of data shall not limit the confidentiality of messages or the protection of privacy any more than is necessary.

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 the Police 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. (343/2008)

(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 the Police. (343/2008)

(4) A telecommunications operator shall immediately notify an Emergency Response Centre, Marine Rescue Coordination Centre, Marine Rescue Sub-Centre and the Police of any disruptions in communications networks, network services and communications services which are significant for the transmission of emergency calls. (343/2008)

(5) Provisions on compensation for costs incurred in fulfilling the obligations provided in subsection 1 above are laid down in section 98 of the Communications Market Act.

Section 35 a (198/2006) - *Obligation of a telecommunications operator to transmit a targeted message from the authorities*

(1) A telecommunications operator is obliged to transmit a targeted message from the authorities, if the message is delivered for transmission by an Emergency Response Centre, a Marine Rescue Coordination Centre or a Marine Rescue Sub-Centre.

(2) Such a targeted message can be sent by an order of the rescue, police or frontier authorities, the Radiation and Nuclear Safety Authority, or the Meteorological Institute, each within their sector. A decision on other targeted communication from the authorities will be made by the competent ministry. A targeted message from the authorities shall be communicated in languages decided by the authorities to terminals and subscriber connections that at the time of the message transmission are located within designated areas. A telecommunications operator shall not change the contents of a message from the authorities.

(3) A targeted alert message shall be transmitted without a delay. Other targeted messages from the authorities shall be transmitted as soon as it is possible without causing unreasonable harm to standard network and communications services.

(4) Provisions on compensation for costs incurred in fulfilling or preparing for the obligations provided in subsections 1–3 above are laid down in section 98 of the Communications Market Act.

(5) The Finnish Communications Regulatory Authority may issue further orders on transmission and response times of and preparatory actions for targeted messages from the authorities referred to in subsections 1–3.

(6) Provisions on alert messages transmitted in television and radio networks and on other messages from the authorities are laid down under section 93 of the Communications Market Act, section 7 of the Act on the Finnish Broadcasting Company Ltd (1380/1993), and section 15 a of the Act on Television and Radio Operations (744/1998).

Section 36 - *Certain other authorities' right of access to information*

(1) The right of authorities to receive identification data for the purpose of preventing, uncovering or investigating crimes is laid down in the Police Act (578/2005), the Act on the Processing of Personal Data by the Border Guard (579/2005), the Customs Act (1466/1994), and the Coercive Measures Act. (343/2008)

(2) Data to be retained under section 14a of this Act is only obtainable from service providers by the authorities who have a legal right to obtain the data from the service provider. (343/2008)

(3) 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 referred to in Chapter 16(9a) of the Penal Code, criminal disturbance referred to in Chapter 17(13)(2) of the Penal Code or breach of domestic peace referred to in Chapter 24(1)(3) of the Penal Code; and (686/2009)

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.

(4) 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 (1061/2006) - *Basis for the payment obligation*

(1) 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.

(2) No information security fee is charged for the turnover from television or radio broadcasting or from retransmission of television or radio broadcasts as referred to in the Act on Television and Radio Operations (744/1998).

(3) If a telecommunications operator discontinues its operations before the end of the payment period, the information security fee shall not be returned.

Section 39 (865/2008) - *Determination of the fee*

(1) The information security fee is determined in payment units according to payment categories. One payment unit equals EUR 60. Telecommunications operators are assigned to payment categories in order to take into account the average costs incurred to the Finnish Communications Regulatory Authority for carrying out the duties related to telecommunications operators of the respective category. The payment category for each operator shall be determined by the turnover that the operator has for telecommunications activities in Finland during the period that precedes the determination of the fee.

(2) The information security fee is determined as follows:

Payment category Turnover (mill. €) Payment units

1 less than 2
2 1-2 4
3 2-4 7
4 4-8 14
5 8-16 26
6 16-32 50
7 32-64 94
8 64-128 179
9 128-192 340
10 192-256 493
11 256-341 645
12 341-427 839
13 427-512 1032
14 512-640 1226
15 640-768 1502
16 768-896 1778
17 896-1024 2054
18 1024-1229 2330
19 1229-1434 2749
20 1434-1638 3169
21 1638-1843 3588
22 1843 or more 4007

In borderline cases the payment of the upper category shall apply.

Section 39 a (1061/2006) - *Turnover as a basis for the payment category*

(1) If a telecommunications operator with turnover from telecommunications is a part of a corporate group as referred to in Chapter 1(6) of the Accounting Act, the basis for the telecommunications operator's fee is the operator's share of the total turnover from telecommunications operations in Finland by the group's liable operators deducted by their mutual turnover from these operations. When the parent company is not Finnish, the basis for the fee remains the same.

(2) If there have been changes in the corporate structure between the end of the previous financial period and the time of issuing the communications market fee decision, the payment category is determined on the basis of the

operator's share of the total turnover from telecommunications operations in the previous closed financial period.

(3) If telecommunications operations have been transferred to another undertaking between the end of the financial period of the previous year and the time of issuing the payment decision, the obligation to pay the fee falls on the undertaking that is involved in public telecommunications at the time of issuing the payment decision. In determining the payment category, the confirmed turnover of the transferred telecommunications operations for the previous closed financial period shall be taken into account.

(4) If the financial period of the telecommunications operator is not 12 months, the turnover will be converted into a sum corresponding 12 months' turnover by multiplying it by 12 and then dividing it with the number of months in the financial period concerned.

Section 40 (1061/2006) - *Stipulating and collecting the information security fee*

(1) The information security fee is collected annually in one instalment. The obligation for an operator to pay an information security fee is stipulated by the Finnish Communications Regulatory Authority. An appeal may be made against a decision of the Finnish Communications Regulatory Authority concerning the stipulation of the fee as laid down in section 43.

(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 due date, annual interest on delayed payments shall 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 interest rate the authority may collect a default payment of five euros if the amount of the interest rate is less than that.

(3) The Act on the Recovery of Taxes and Fees by Recovery Proceedings (367/1961) has been repealed by the Act on implementing taxes and fees (706/2007).

Section 40 a (1061/2006) - *Submittal of data to the Finnish Communications Regulatory Authority and payment obligation in certain exceptional circumstances*

(1) For the purpose of determining a fee the Finnish Communications Regulatory Authority has the right to obtain from telecommunications operators turnover data from the period preceding the determination of the fee. Operators that are part of a group shall also give an account of the instalments from the group's mutual telecommunications operations that have been deducted from the telecommunications turnover under section 39 a(1). A telecommunications operator shall submit the information to the Finnish Communications Regulatory Authority within one month of the adoption of the financial statement. A copy of the adopted financial statement and the group financial statement shall be submitted as an attachment.

(2) If no sufficiently reliable account of the turnover is available due to missing financial statements or some other comparable, especially weighty reason, the Finnish Communications Regulatory Authority's estimate of the turnover may be used as the basis for the payment. In the estimate due consideration must be given to:

1) telecommunications operator's extent of operations;

2) telecommunications operator's position on the market;

3) data about the telecommunications operator's services, number of clients and invoicing;

4) reference data about other telecommunications operators providing similar services; and

5) other similar elements affecting the telecommunications operator's turnover.

(3) Before taking the measures referred to in subsection 2 the Finnish Communications Regulatory Authority shall ask the telecommunications operator to submit the information needed for determining the information security fee within a reasonable period on pain of the Finnish Communications Regulatory Authority estimating the turnover.

Chapter 11 - *Miscellaneous provisions*

Section 41 - *Coercive measures*

(1) If anyone violates this Act or provisions issued under it and, despite being requested to do so, fails to rectify his or her 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 his or her error or neglect. 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.

(4) The Act on the Recovery of Taxes and Fees by Recovery Proceedings (367/1961) has been repealed by the Act on implementing taxes and fees (706/2007).

Section 42 (125/2009) - *Penal provisions*

(1) The penalties for communications secrecy violation and aggravated communications secrecy violation are provided in Chapter 38(3 and 4) of the Penal Code, and the penalty for unauthorised access to data in Chapter 38(8) of the Penal Code. The penalty for a breach of the obligation of secrecy provided in section 5 of this Act is subject to Chapter 38(1 or 2) of the Penal Code, unless the offence is punishable under Chapter 40(5) of the Penal Code

or unless a more severe penalty is provided elsewhere. A breach of the confidentiality requirements laid down in section 13 h(3) shall be punished pursuant to Chapter 38(2)(2) of the Penal Code unless a more severe penalty than in section 38(1) of the Penal Code is laid down elsewhere in law.

(2) Anyone who deliberately

1) violates the prohibition on the possession, importing, manufacture or distribution of any system or part of a system 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 in section 21(1) or section 35(4); (365/2011)

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; or

9) neglects to comply with the provisions of 13g–13i regarding drawing up and issuing a report or a prior notification to the user, the employees' representative or the Data Protection Ombudsman

shall be imposed a fine for a *violation of protection of privacy in electronic communications*, unless a more severe penalty is provided elsewhere in law.

(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 its 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.

****

Application and entry into force of amendment provisions
15.7.2005/599:
This Act enters into force on 1 September 2005.

17.3.2006/198:
(1) This Act enters into force on 1 April 2006.

(2) Measures necessary for the implementation of this Act may be undertaken before the Act's entry into force.

1.12.2006/1061:
This Act enters into force on 1 January 2007.

9.2.2007/144:
This Act enters into force on 15 February 2007.

21.12.2007/1328:
This Act enters into force on 1 January 2008.

23.5.2008/343:

(1) This Act enters into force on 1 June 2008.

(2) Measures necessary for the implementation of this Act may be undertaken before the Act's entry into force.

(3) A service provider shall retain data concerning e-mail services and internet phone services in accordance with this Act as of 15 March 2009 the latest.

19.12.2008/865:

(1) This Act enters into force on 1 January 2009.

(2) Measures necessary for the implementation of this Act may be undertaken before the Act's entry into force.

(3) In 2009 and 2010, however, the information security fee is defined as follows:

Payment category Turnover (mill. €) Payment units in 2009 Payment units in 2010
1 less than 1 2 2
2 1-2 4 4
3 2-4 7 7
4 4-8 14 14
5 8-16 26 26
6 16-32 50 50
7 32-64 94 94
8 64-128 179 179
9 128-192 340 340
10 192-256 390 441
11 256-341 645 645
12 341-427 709 773
13 427-512 773 900
14 512-640 1226 1226
15 640-768 1317 1408
16 768-896 1408 1590

17 896-1024 1499 1772
18 1024-1229 2330 2330
19 1229-1434 2468 2607
20 1434-1638 2607 2884
21 1638-1843 2745 3160
22 1843 or more 2883 3437

13.3.2009/125:
This Act enters into force on 1 June 2009.

11.9.2009/686:
This Act enters into force on 1 November 2009.

8.4.2011/365:
This Act enters into force on 25 May 2011.