

**EXPLANATORY NOTES TO REGULATION 9
ON THE OBLIGATION TO NOTIFY OF
VIOLATIONS OF INFORMATION
SECURITY IN PUBLIC
TELECOMMUNICATIONS**

CONTENT

CONTENT 1

1 LEGAL MATTERS 2

1.1 Legislative basis for the regulation 2

1.2 Other related provisions..... 2

 1.2.1 *Other legislation* 2

 1.2.2 *FICORA's technical regulations* 3

 1.2.3 *Handling of notified data at FICORA* 4

2 THE OBJECTIVE OF THE REGULATION AND THE CHANGES MADE TO IT 5

2.1 The objective of the regulation 5

2.2 Key changes and changes made in the past..... 5

3 SECTION-SPECIFIC BASIS AND GUIDELINES FOR APPLICATION..... 6

3.1 Section 1 Scope of application 6

 3.1.1 *Reasons and scope of application* 6

3.2 Section 2 Notifying subscribers 7

 3.2.1 *Reasons* 7

 3.2.2 *Application*..... 7

3.3 Section 3 Notifying FICORA 8

 3.3.1 *Reasons* 8

 3.3.2 *Application*..... 8

4 OTHER RECOMMENDATIONS..... 11

4.1 Recommendation on cooperation in the event of a violation of information security 11

4.2 Recommendation on notifying FICORA of information security situations..... 11

4.3 Recommendation on notifying of violations against others than telecom operators 11

5 REFERENCES..... 12

1 LEGAL MATTERS

The aim of this chapter is to give the reader of the regulation a general overview of the provisions this regulation is based on. In addition, the chapter explores other substantial legislation in this respect.

1.1 Legislative basis for the regulation

FICORA's regulation relies on section 21 of the Act on the Protection of Privacy in Electronic Communications (516/2004, PPEC) [1]. The Act on the Protection of Privacy in Electronic Communications, which entered into force on 1 September 2004, gave, for its part, effect to the *Directive on privacy and electronic communications* [2] adopted by the EC in July 2002.

Pursuant to section 21(1) of the PPEC, a telecommunications operator must immediately notify the subscriber of a threat to information security of a service and report the following:

- measures available to subscribers and users for combating the threat; and
- the probable costs of such measures.

Under section 21(2) of the PPEC, telecommunications operators 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. Notification must also be made of measures undertaken to prevent the reoccurrence of such violations of information security, threats of such violations. After 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.

Pursuant to section 21(4) of the PPEC, FICORA may issue telecom operators:

- further regulations on the content and form of notifications to be submitted of a specific threat to the information security to subscribers;
- regulations on significant violations of information security and threats of such violations in services and on the content, form and delivery to FICORA of the notification submitted to FICORA; and
- guidelines on the content and form of the publication of information after having removed a significant information security violation or threat.

1.2 Other related provisions

1.2.1 Other legislation

Section 19 of PPEC — Obligation to maintain information security. According to the section, a telecommunications operator must maintain the information security of its services. Maintaining information security in such services 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. The obligation to maintain information security also concerns the handling of data necessary for the purpose of carrying out the obligation to store identification data. Telecommunications operators are responsible to subscribers and users for the information security also on the behalf of any third party that wholly or in part provides a network service, communications service, storage of data or value added service.

Section 20 — Measures taken to implement information security. According to the section, a telecom operator and any party acting on its behalf has the right to undertake necessary measures in order to ensure information security in the following situations:

- 1) for the purpose of detecting, preventing, solving and bringing to pre-trial investigation disturbances causing harm to the information security of communications networks and related services;
- 2) for the purpose of ensuring the communications possibilities of the sender or recipient of the message; or
- 3) for the purpose of preventing the preparation of means of payment fraud referred to in section 37(11) of the Penal Code [3] to be implemented via communications services on a large scale.

The necessary measures in order to ensure information security may consist of:

- 1) an automatic analysis of the content of the message;
- 2) an automatic prevention or restriction of the delivery or reception of messages;
- 3) an automatic removal of malicious software endangering information security from messages; and
- 4) any other comparable technical measures.

If the type or form of message or equivalent gives reason to believe that the message contains a malicious program or command, and an automatic analysis of the content of the message is unable to ensure that the objections referred to in *section 20 of the PPEC* can be reached, the content of a specific message may be handled manually. The sender and receiver of the message must be notified if the content of a message is handled manually, unless the notification is likely to endanger the realization of objectives. Telecom operators must realise any measures 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 ensuring the objectives of the handling. Such measures must be discontinued immediately if the conditions for them specified in this section no longer exist.

Communications Market Act (393/2003, CMA) [4], section 131, *Obligation to eliminate interference*. According to the section, if a communications network or equipment item causes danger or interference to a communications network, equipment, communications network user or another person, the telecommunications operator or the keeper of another communications network or equipment shall take measures immediately to rectify the situation and, if necessary, isolate the communications network or equipment from the public communications network.

1.2.2 FICORA's technical regulations

Regulation 11 *on information security and functionality of e-mail services* [5]. The regulation applies to the production of e-mail services provided in public communications networks and to the systems, communications networks and services used by an e-mail service provider for this purpose. The aim of the regulation is to ensure that the e-mail services used by consumers are effective.

Regulation 13 *on information security and functionality of Internet access services* [6]. The regulation applies to the production of Internet access services provided in public communications networks and to related systems, communications networks and communications services used by telecommunications operators to provide these services. In the regulation, Internet access service means transmission of Internet traffic. The regulation applies, as applicable, also to the production of Internet access services both for network operators and for service operators.

Regulation 47 *on information security of telecommunications operators* [7]. The regulation is applied to activities related to the implementation of public network and communications services of telecom operators. The regulation's scope of application covers, for example, the provision of internet access services, e-mail services and voice services referred to in the Communications Market Act. The regulation is also applied to telecommunications operations of minor significance. The regulation imposes information security requirements to be taken into consideration in the activities of telecom operators.

Regulation 57 *on the maintenance of communications networks and communications services and procedures in the event of faults and interference* [8]. The regulation applies to all public communications networks and communications services provided therein. The objective of the

regulation is to improve the readiness of telecom operators in the event of faults and disturbances as well as related readiness procedures.

The list corresponds to the situation at the time this document was published. FICORA's regulations are available at FICORA's website at www.ficora.fi.

1.2.3 Handling of notified data at FICORA

FICORA handles the information submitted to it under section 21 of the PPEC in a confidential manner. Pursuant to the *Act on the Openness of Government Activities* (621/1999) [9], the information is secret.

- According to section 24(1)(7) of the Act on the Openness of Government Activities, unless otherwise provided, public documents to be kept secret are documents relating to or affecting the realisation of the security arrangements of persons, buildings, installations, constructions, and data and communications systems, unless it is obvious that access will not compromise the achievement of the objective of the security arrangements.
- According to *section 24(1)(20) of the Act on the Openness of Government Activities*, documents containing information on a private business or professional secret, as well as documents containing other comparable private business information, if access would cause economic loss to the private business, provided that the information is not relevant to the safeguarding of the health of consumers or the conservation of the environment or for the promotion of the interest of those suffering from the pursuit of the business, and that it is not relevant to the duties of the business and the performance of those duties, are also to be kept secret.

According to section 34 of the PPEC, FICORA is entitled to disclose identification data in connection with collecting information on and investigating violations of information security, on certain conditions, to those telecommunications operators, value added service providers and corporate 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 or are likely to be subject to such a violation of information security. In addition, FICORA is entitled to disclose the identification data in connection with collecting information on and investigating violations of information security to a foreign authority or other party who is responsible for the prevention of or investigation of violations of information security to communications networks or communications services.

However, FICORA is entitled to disclose the identification data only to the extent necessary to prevent and clarify violations of information security. The disclosure of data must not limit the confidentiality of a message and protection of privacy any more than is necessary.

2 THE OBJECTIVE OF THE REGULATION AND THE CHANGES MADE TO IT

The aim of this chapter is to give the user of the regulation information on the objectives and aims of the regulation. This chapter also includes the most important changes made to the obligations and recommendations preceding the regulation.

2.1 The objective of the regulation

The objective of the regulation is to define the content and measures of the notifications submitted to FICORA and subscribers concerning a significant violation of information security or threat to it referred to in section 21 of the Act on the Protection of Privacy in Electronic Communications.

2.2 Key changes and changes made in the past

Re-grouping of regulations:

In the beginning of 2010, in connection with the regulation reform, provisions concerning the telecom operators' obligation to notify of faults and disturbances included in regulation 9 will be transferred to a new regulation 57 on the maintenance of communications networks and communications services and procedures in the event of faults and disturbances.

The notification obligation concerning violations of information security which remains in regulation 9 will not undergo significant changes. However, it now has separate sections for notifying subscribers and FICORA. In addition, the explanatory notes to the regulation now have a recommendation on cooperation between telecom operators in the event of a violation of information security.

3 SECTION-SPECIFIC BASIS AND GUIDELINES FOR APPLICATION

This chapter examines the basis for each section and the guidelines for their application.

3.1 Section 1 Scope of application

3.1.1 Reasons and scope of application

Public telecommunications:

The scope of application of the regulation includes the public telecommunications of telecom operators. Public telecommunications means the provision of a network service or a communications service to a set of users that is not subject to any prior restriction. *Network service* means a network operator's service that is in its ownership or for other reasons in its possession for the purposes of transmitting, distributing or providing messages. Whereas a communications service means a service operator's service including the transfer of messages in a communications network in the possession of the operator or leased from a network operator, or delivery of or provision of messages in a mass communications network.

Section 2 of the CMA defines a communications network, which refers to networks provided for both targeted communications and mass communications. Thus, the Regulation is applicable to e.g. fixed and wireless telephone and data network, cable television network, and on certain conditions, terrestrial digital television network and analogue radio. What is relevant with the definition of a public communications network is that the network is provided to a set of users that is subject to prior restriction. What is relevant with the definition of a communications service is that a telecom operator, as a service provider, participates in the transmission of the messages or the provision of them.

The regulation is also applied to telecommunications of minor importance that is not subject to the telecommunications notification obligation pursuant to section 13 of the CMA. However, the regulation does not apply to content services or services provided to a set of users that is subject to prior restriction.

Definition of the application of mass communications networks

The PPEC or the regulation do not apply to messages transmitted over a mass communications network if the message cannot be associated with an individual subscriber or user receiving it. Thus, the regulation is applied to mass communications networks only if they are used for other purposes than television and radio operations.

According to the Communications Market Act, *mass communications network* means a communications network primarily used for broadcasting or providing television and radio programmes or other material transmitted in identical form to all recipients. A 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. The concept of a message also includes such messages with content that are delivered to unspecified recipients, such as television programmes and radio programmes and all information delivered via websites open to the public of electronic communications networks.

Public authority networks:

The regulation does not either 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. In the Communications Market Act, a public authority network means a communications network built for the needs of public order and security, rescue activities or civil defence, whose subscriber connections can be made available not only to public authorities but also to other user groups essential to the discharging of the duties referred to above. According to the CMA, a public authority network can be a so-called pure

dedicated network, or it can be connected to a public communications network when calls can be made from the public authority network to a public telephone network.

However, the regulation is applied to other public telecommunications than the activities of a public authority in public authority networks.

3.2 Section 2 Notifying subscribers

3.2.1 Reasons

Ensuring the necessary prerequisites for the subscribers and users of the services provided by telecom operators requires that subscribers and users are aware of the information security risks to the service. According to the Act on the Protection of Privacy in Electronic Communications, *if a specific threat applies to the service and service providers are unable to solve it on their own or together with other players, the service provider must immediately notify subscribers of any delay in service. In addition, the operator must also notify the measures available to subscribers and users for combating the threat, and the probable costs of such measures.*

3.2.2 Application

Assessment of a specific threat

Examples of specific information security threats to be notified to subscribers can be:

- up-to-date information security threats at the time and combating against them with regard to terminal devices and software related to the use of the internet
 - threats related to malware and how they spread, for example, via e-mail, websites, mobile devices and peer-to-peer networks
 - rerouting of (call) number information of modem-based internet traffic
- serious defects detected in the information security of publicly-available systems and software, for example, unpatched, widely-known vulnerabilities in software or systems (information available from CERT alerts or from the system provider)
- up-to-date information security threats related to the use of communications services requiring special attention from the users of communications services
 - wide-scale malware epidemics requiring immediate action from subscribers
 - significant increase in the number of spam messages, which affects the availability of e-mail services
 - other such occurrences in communications networks that significantly risk the information security and protection of subscribers
- specific threats caused by the international nature of communications services
 - information security threats to a communications service targeted towards users in Finland resulting from the fact that the service is partially or entirely provided outside Finland, and which the telecom operator is not able to prevent by own means

It is recommended that notifications of software vulnerabilities are given if an unpatched vulnerability found in publicly-used software is particularly easily exploitable and thus threatens the information security of networks and services in general.

Timing of the notification

Some of the threats to the service of a telecom operator are of the type that it is not immediately possible to patch them. Issuing public notifications of such threats would endanger the confidentiality of communications or enable large-scale economic frauds. The primary measures to combat such threats would be to patch the vulnerability in order to avoid any additional damage to subscribers.

According to the PPEC, *after 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.* The nature of notifications must be general and specifically after-action. However, it is necessary to notify of the

measures in as up-to-date manner as possible. Subsequent notifications improve the possibilities of a player, who is the subject of the violation of information security or threat, to react in situations requiring after-action measures.

Notification procedures

Examples of suitable communications channels are the telecom operators' websites, information bulletins sent along with the invoice and e-mail messages. Websites and information bulletins have excellent suitability for, for example, in such cases where the threat is not critical and does not require immediate measures from the subscriber. These are, for example, bulletins concerning general threats to the use of the internet and measures available to combat them. Websites are also suitable for notifying of more critical threats, for example, acute dangerous growing malware traffic in communications networks. Sending the notification by e-mail is suitable in cases where the threat only concerns a limited number of telecom operators' subscribers and where notifying other than the parties concerned would risk the information security or protection of the subscribers. The use of mass communications media as a communications channel can be justified in critical, large-scale situations.

It is advisable that a customer notice giving basic instructions on how to prevent a typical internet user's information system from the most imminent threats of the use of the internet should be attached to the material given to the subscriber in connection with the opening of the subscription. The guidelines should be renewed regularly, for example, once a year, in connection with the supplementary material sent to the subscriber.

The telecommunications operator must inform the subscriber if his or her subscription has been disconnected due to information security problems in the subscription. The subscriber must be notified of the telecom operator's measures to rectify the situation and of the measures the telecom operator expects the subscriber to take in order to rectify the information security of the subscription.

Recommendation

In addition, FICORA recommends that the telecom operator notifies its customers of the most typical scam/fraud attempts related to the use of communications services, and of the correct manner to react to them, for example:

- SMS requests from unknown number to call back to additional-cost services;
- ghost calls aiming at rebound calls from additional-cost or foreign numbers; and
- up-to-date phishing attack campaigns.

3.3 Section 3 Notifying FICORA

3.3.1 Reasons

The information requested in the notification on information security violations are needed for the establishment of controlled, up-to-date and analysed overview of the information security situation of national communications networks and services. The up-to-date information enables that counter-measures can be directed and emphasized. In addition, drafting a notification helps the organization to follow the management process of its information security and establish an overview of the organization-specific information security. The requested information are basic information needed for the analysis of information security incidents.

3.3.2 Application

Under the PPEC, telecommunications operators 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. *Telecom operators must notify FICORA of measures undertaken to prevent the reoccurrence of such violations of information security, threats of such violations.*

Assessment of significance

When assessing the significance of a violation, the threat of it and fault or disturbance, according to PPEC, attention must be paid to the protection of the rights of the subscribers and users, availability of the service and the scope of geographic effects. The notification must be made immediately after the significance has been identified. The notification must clearly indicate what measures have already been taken and, if possible, how the problem can be avoided in the future. If, in the connection of the notification, it is not possible to state what action should be taken in the future, the notification must be completed without delay.

The list depicts examples of such cases of which a notification must be made. The list is not exhaustive, but it aims at depicting the severity level of the threshold of submitting a notification. Examples of violations of information security to be notified to FICORA are:

- break-ins to a telecom operator's information systems;
- violations of information security to the telecom operator's information system;
 - identification, customer and configuration data falls into wrong hands;
 - network documentation data or structure descriptions fall into wrong hands;
 - unauthorized access to the system as main user;
 - unauthorized access into the system by using a user name that allows access to the content of the communication or identification data or allows to adjust the configurations of the telecom operator's information systems and communication systems;
- violations of information security with significant impact on the availability of communications networks or services;
 - denial-of-service attacks;
 - sudden increase in the amount of e-mail spam;
 - attacks affecting the routing of communications network traffic;
- activation of malware (e.g. computer viruses, backdoor installation programs, "Trojans", spyware or sniffer programs) in the telecom operator's information systems;
- attempts to obtain information endangering the information security of a telecom operator or its customers from the personnel of the telecom operator (so-called "social engineering");
- detected tapping, monitoring devices, installations and software in the communications network or in the information systems or facilities of the telecom operator;

The list depicts examples of such cases of which a notification must be made. The list is not exhaustive, but it aims at depicting the severity level of the threshold of submitting the notification. Examples of information security threats to be notified to FICORA are:

- Detected, significant data system break-in attempts
 - systematic attempts, deviating from normal use of the network, with the purpose to find out, by means of technical measures, information about the following features of communications networks and services;
 - the physical and logical topology of the network;
 - hardware and software versions;
 - eventual vulnerabilities in the systems;
 - systematic, hostile log-in attempts into the information systems of telecom operators;
 - a data break-in attempt into a component belonging to priorities 1 and 2 referred to in FICORA's regulation 54/2008 on the routing and ensuring emergency traffic;
- network traffic that deviates from normal;
 - large amount of traffic directed at unused network address blocks;
 - unknown or rarely-used protocol have substantial traffic volumes;
 - sudden increase in rare foreign destinations;
- significant information security flaws a telecom operator has detected in information systems and software that have not been made public in a CERT alert or on behalf of the system manufacturer;
 - security loopholes that enable unauthorized access as the main user of the system;
 - security loopholes enabling unauthorized access into the content of the communication or identification data or allow to adjust the configurations of the telecom operator's information systems and communication systems;

- large-scale spreading or activation of malware in communications networks causing significant threat to the services of telecom operators and customers;
- specific threats caused by the international nature of communications services;
 - detection of an information security threat to a communications service targeted towards users in Finland resulting from the fact that the service is partially or entirely provided outside Finland, and which the telecom operator is not able to prevent by own means.

Notification procedures

If a violation of information security or information security threat is serious, there is reason to suspect that the message delivery system used for submitting the notification has a violation of information security, or the situation call for immediate measures from FICORA, the first notification should be made on the telephone based on existing information. A further notification in writing may be submitted, when it is possible to make a more detailed overview. In long-term cases, the telecom operator must keep FICORA up-to-date on how the situation develops. An electronically-submitted notification that can be produced in a form that is written and readable, is deemed to be written.

A recommended way to notify is to use the form in annex 1 for the purpose of notifying of violations of information security and information security threats. The notification can also be made by e-mail, for example. The text to be used can be free-form, if it delivers the information content of the form.

Telecom operators are requested to notify FICORA and keep up to date their contact information with regard to the handling functions of violations of information security and control rooms by using the form referred to in annex 2.

Contact details

E-EMAIL: CERT@FICORA.FI

Information on the PGP keys of the CERT-FI unit for the purpose of encrypting e-mail messages are available at <https://www.cert.fi/en/activities/contact/pgp-keys.html>.

Telephone: +358 9 6966 510
Telefax: +358 9 6966 515

Postal address:
Finnish Communications Regulatory Authority
CERT-FI
P.O. Box 313
FI-00181 HELSINKI

4 OTHER RECOMMENDATIONS

4.1 Recommendation on cooperation in the event of a violation of information security

FICORA recommends that telecom operators have active cooperation both among themselves and with FICORA's CERT-FI unit for detecting violations of information security and information security threats.

It is recommended that units responsible for telecom operators' network management and detection of violations of information security notify other telecom operators, too, of such violations of information security and information security threats affecting or that may affect the communications network or service of another telecom operator.

4.2 Recommendation on notifying FICORA of information security situations

FICORA recommends that players notify, at their own discretion, CERT-FI also of violations of information security of lesser importance and information security threats of lesser importance. The information supports the establishment of the national overview of information security and help CERT-FI develop its services according to the needs of the players.

4.3 Recommendation on notifying of violations against others than telecom operators

FICORA recommends that also other players than telecom operators notify FICORA's CERT-FI unit of violations of information security against them and of information security threats. For example, CERT-FI can help and support the player that is the target of the attack in recovery from the attack and eventual counter-measures. In addition, CERT-FI has an extremely wide international cooperation network which enables that international information security situation can be addressed quickly and efficiently.

5 REFERENCES

- [1] Act on the Protection of Privacy in Electronic Communications (516/2004): <http://www.finlex.fi/en/laki/kaannokset/2004/en20040516.pdf> (amendments up to 1328/2007 included)
- [2] Directive 2002/58/EC of the European Parliament and of the Council on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), 7 March 2002. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:FI:NOT>
- [3] The Penal Code (39/1889 incl. amendments, CMA), updated version: <http://www.finlex.fi/pdf/saadkaan/E8890039.PDF> (amendments up to 650/2003 included)
- [4] Communications Market Act (393/2003 incl. amendments, CMA), updated version: <http://www.finlex.fi/fi/laki/kaannokset/2003/en20030393.pdf> amendments up to 119/2008 included
- [5] FICORA 11A/2008 M, on information security and functionality of e-mail services <http://www.ficora.fi/attachments/englantiav/5B37cMfzM/FICORA11A2008M.pdf>
- [6] FICORA Regulation 13 A/2008 M on information security and functionality of Internet access services, <http://www.ficora.fi/attachments/englantiav/5B37hthyt/FICORA13A2008M.pdf>
- [7] FICORA Regulation 47 C/2009 M on information security management of telecommunications operators <http://www.ficora.fi/attachments/englantiav/5k8y6zm5w/FICORA47C2009M.pdf>
- [8] FICORA Regulation 57/2009 M on the maintenance of communications networks and services and procedures in the event of faults and interference
- [9] Act on the Openness of Government Activities (621/1999 amendments up to 1060/2002 included): <http://www.finlex.fi/en/laki/kaannokset/1999/en19990621.pdf>