FINLAND – COUNTRY REPORT

Background

This report outlines the main laws which provide law enforcement and intelligence agencies with legal powers in relation to lawful interception assistance, the disclosure of communications data, certain activities undertaken for reasons of national security or in times of emergency, and censorship of communications under Finnish law.

ELECTRONIC COMMUNICATIONS SERVICES ACT 157§: DATA RETENTION

(laki sähköisen viestinnän palveluista 157§)

The obligation to retain data concerns only companies separately designated by decisions of the Ministry of the Interior. Ministry of the Interior has separately 27.2.2015 designated by its decision that DNA Oyj, Elisa Oyj, Telia Finland Oyj ja Ålands Telekommunikation Ab are telecommunications operators under the retention obligation.

The retention obligation concerns only services that the operator under the said obligation itself provides, and it does not obligate operators to collect or retain any new data. The sole purpose is to extend the retention time for data that operators already process for the purposes of providing their own services.

Data under the retention obligation is retained solely for the purposes of the authorities and may be used only for the purposes of solving and considering charges for certain specified criminal acts of the Coercive Measures Act (806/2011).

Service	**Data to be retained**	**Retention period** (the data retention time starts with the time of the communications)
a telephone service or SMS service	• name and address of a registered user or a subscriber • subscription identifier and data that can be used to identify a communications service user or communications • recipient of the communications, the type, receiver, time and duration of communications (including call transfers) • data that can be used to identify the device used and the location of the device and the subscriber connection it uses in the beginning of communications	**12 months**
Internet telephone service	• name and address of a registered user or a subscriber • subscription identifier and data that can be used to identify a communications service user or communications • recipient of the communications, the type, receiver, time and duration of communications (including call transfers)	**6 months**

Service	Data to be retained	Retention period (the data retention time starts with the time of the communications)
Internet access service	• name and address of a registered user or a subscriber • subscription identifier, installation address, and data that can be used to identify the communications service user, • the device used in communications and the time and duration of the service	**9 months**

ELECTRONIC COMMUNICATIONS SERVICES ACT 158§: OBLIGATIONS AND PROCEDURES FOR PROCESSING DATA RETAINED FOR THE PURPOSES OF THE AUTHORITIES

The operators under the retention obligation have the obligation to maintain the information security of the data to be retained on the basis of the retention obligation.

The operator under retention obligation decides on the technical implementation of the retention. It must be ensured that the data retained can be transmitted to the authorities entitled to it without undue delay.

Obligations relevant for the implementation of the retention obligation are particularly contained in chapter 2 of Traficom Regulation 67 (Information security in telecommunications operations) on the general requirements of all networks and services.

Traficom Regulation 53 (on the data retention obligation of telecommunications operators for the purposes of the authorities) defines the technical details of the data covered by the retention obligation and specify the technical implementation of the retention and the information security requirement concerning the data retention under section 158§.

COERCIVE MEASURES ACT (806/2011) AND POLICE ACT (872/2011).

The most important Acts related to the right to obtain data covered by the retention obligation are the chapter 10 of the Coercive Measures Act and chapter 5 and 5a of the Police Act.

A general prerequisite for the use of covert coercive measures is that their use may be assumed to produce information needed to clarify an offence, and measures are used in the investigation of crimes and other secret means of gathering intelligence to try to prevent or detect crimes or avoid danger. These measures include e.g. interception and monitoring of telecommunications.

For purposes of legal protection, it is thought important to adhere to the principle that interception of telecommunications and, in most cases, remote surveillance may only be employed with a court's permission on the request of an official with the power of arrest. The warrant for telecommunications interception and for obtaining the other corresponding information may be given for at most one month at a time.

There is an exception to the general rule. If the matter does not brook delay, an official with the power of arrest may decide on traffic data monitoring and on the obtaining of location data until such time as the court has decided on the request for the issuing of the warrant. The matter shall be submitted for the decision of the court as soon as possible, but at the latest within 24 hours of the initiation of the use of the coercive measure. The warrant may be issued and the decision may be made for at most one month at a time and the warrant or decision may be issued to extend also to the period prior to the issuing of the warrant or the making of the decision, which may be longer than one month.

The National Police Board and the chiefs of units using covert coercive measures supervise the use of covert coercive measures on the part of the police. The Ministry of the Interior shall submit an annual report to the Parliamentary Ombudsman on the use and supervision of covert coercive measures and their protection.

CIVILIAN INTELLIGENCE LEGISLATION

Finland adopted civilian intelligence legislation in June 2019. Provisions on human intelligence and information systems intelligence were issued in the new chapter 5a of Police Act. The civilian intelligence powers may be used only by the Finnish Security and Intelligence Service, and they can also be exercised abroad. Information gathering by the Finnish Security and Intelligence Service will aim not only to prevent and detect crime but also to safeguard national security.

MILITARY INTELLIGENCE LEGISLATION (2019/590) "LAG OM MILITÄR UNDERRÄTTELSEVERKSAMHET"

Finland adopted military intelligence legislation 2019, the purpose of military intelligence is to obtain and process information on military activities focusing on Finland or important to Finland's security environment. The act contains provisions on military intelligence authorities' cooperation with other authorities, international cooperation and prohibitions

on intelligence gathering and data processing. Military intelligence authorities include the Defence Command of the Defence Forces and the Defence Force Intelligence Agency. The authorities have these powers both in Finland and abroad. Provisions on military intelligence in telecommunication networks were issued in the chapter 4 of Military Intelligence Act.

COSTS

According to Electronic Communications Services Act 299§ telecommunications operator has the right to receive compensation from State funds for the direct costs of the investment and maintenance of systems, equipment and software acquired for the sole purpose of assisting public authorities. Compensation shall be payable by the authority for which the acquisition was made.

According to Coercive Measures Act section 64 and Police Act section 62, a telecommunications operator has the right to compensation from state funds for the direct expenses of assistance to the authorities referred to in this Chapter and of providing information as provided in Electronic Communications Service Act. The criminal investigation authority unit that conducted the investigation decides on the payment of the compensation.