EUROPEAN
JUDICIAL NETWORK

Fiches Belges on electronic evidence - Answers of Finland

1. Definition of electronic evidence

Electronic evidence has not been defined in our legislation. Law enforcement authorities can obtain any kind of evidence by using different coercive measures possible by law or by requests to service providers. That evidence can also be in a form of an electronic data.

2. Which measures are possible in your Member State under International Judicial Cooperation?

Law enforcement authorities can:
- make a request for information to service providers
- confiscate/copy a document
- make a search of data contained in a device/remote search
- request a warrant for a traffic data monitoring
- request a warrant for a telecommunications interception

In relation to EU Member States Finland applies the Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO) and its implementing legislation. In relation to certain questions, the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union is also applied.

In relation to other states a Finnish authority grants mutual legal assistance as provided for in the Act on International Judicial Assistance in Criminal Matters (4/1994) or as agreed with a foreign country. The most important conventions are the European Convention on Mutual Legal Assistance in Criminal Matters and the Second Additional Protocol thereto.

3. Procedure for obtaining electronic evidence

a. National procedures

According to the Coercive Measures Act (of Finland) coercive measures may only be used when they may be deemed justifiable with consideration to seriousness of the offence under investigation, the importance of clarifying the offence, the degree to which the use of the coercive measures infringes on the rights of the suspect in the offence or of others and the other circumstances in the case. Comprehensive provisions on covert coercive measures for the investigation of an offence are stipulated in Chapter 10 of the Coercive Measures Act.

A request to ISP:
According to the Police Act, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members and employees of an organisation.

A commanding police officer must make the request.

Confiscation a document:

According to the Coercive Measures Act, a document may be confiscated if there are grounds to suspect that:

- it may be used as evidence in a criminal case;
- it has been taken from someone in an offence; or
- it may be ordered forfeited.

The same conditions also apply to information that is contained in a technical device or in another corresponding information system or in its recording platform (*data*).

An official with the power of arrest decides on confiscation or copying of a document. The court may decide on this when considering the charges.

A search of data contained in a device/remote search:

Law enforcement authorities are empowered also to make a search of data contained in a device.

A search may be conducted if:

- there is reason to suspect that an offence has been committed and the most severe punishment provided for the offence is imprisonment for at least six months, or if the matter being investigated involves circumstances connected to the imposition of a corporate fine; and
- it may be presumed that the search can lead to the discovery of a document or data to be confiscated or to a document to be copied and that is connected with the offence under investigation.

When required by the appropriate conduct of a criminal investigation or by the urgency of the matter, a search of data contained in a device may be conducted as a remote search.

> *Definition of a remote search= the search of data is conducted without using the device that is in the premises or in the possession of the person who is the subject of the search.*

An official with the power of arrest decides on a search of data contained in a device. In an urgent situation a police officer may make the decision.

A warrant for a traffic data monitoring

A criminal investigation authority may be issued a warrant for traffic data monitoring of a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect the said person of an offence listed in the Coercive measures Act (of Finland). (Please see more detailed in question 7 *regarding definition of data categories and examples: subscriber, traffic/transaction and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations).*

The court decides on traffic data monitoring referred on the request of an official with the power of arrest.

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 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.

A warrant for a telecommunications interception

A criminal investigation authority may receive permission for telecommunications interception directed at a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect him or her of an offence listed in the Coercive Measures Act (of Finland). (Please see more detailed in question 7 *regarding definition of data categories and examples: subscriber, traffic/transaction and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations)*.

The court decides on telecommunications interception on the request of an official with the power of arrest.

The warrant for telecommunications interception may be given for at most one month at a time.

b. international procedures (including Available channels/ways to obtain electronic evidence from your Member State; urgent procedures; specialised networks to obtain electronic evidence e.g. 24/7 Budapest Convention/police channels)

In Finland, our Communication Centre (located at National Bureau of Investigation) handles all incoming requests 24/7. Communication Centre is also our SPOC for Budapest Convention. We also use Siena- and Interpol channels to receive any types of requests. All urgent requests to Finland should be pointed to Communication Centre by using Interpol, Siena or SIRENE channels.

4. International legal framework applicable for this measure in your Member State

Main instruments:

- European Investigation Order (EIO)
- Budapest Convention
- Bilateral treaties or police-to-police cooperation within their own legal framework.

Evidence can also be gathered by using different applicable international treaties. The use of an applicable treaty depends on the requesting State.

5. Competent authority to receive and execute your request

- National Bureau of Investigation Finland

6. Accepted languages

- Finnish
- Swedish
- English

7. Definition of data category and examples: subscriber, traffic/transaction and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations

Subscriber data:

In individual cases, the police has the right to obtain from a telecommunications operator and a corporate or association subscriber on request contact information about a network address that is not listed in a public directory or data identifying a network address or terminal end device if the information is needed to carry out police duties. Similarly, the police has the right to obtain postal address information from organisations engaged in postal services (The Police Act Chapter 4, Section 3 paragraph 2).

Traffic data:

Traffic data monitoring refers to

- the obtaining of **identifying data regarding a message** that has been sent from or received by a network address or terminal end device connected to a telecommunications network,
- the obtaining of **location data** regarding the network address or the terminal end device, or
- the **temporary prevention of the use** of the network address or terminal end device.

Identifying data refers to data that can be connected to the subscriber or user and that is processed in telecommunications networks in order to transmit or distribute messages or keep messages available.

A criminal investigation authority may issue a warrant for traffic data monitoring of a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect the said person of:

(1) an offence for which the most severe punishment is imprisonment for at least four years;
(2) an offence committed with the use of the network address or terminal end device, for which the most severe punishment provided is imprisonment for at least two years;
(3) unauthorized use, damage to property, message interception or computer break-in directed at an automatic data processing system and committed with the use of a network address or terminal end device;
(4) exploitation of a person subjected to the sex trade, solicitation of a child for sexual purposes or pandering;
(5) a narcotics offence;
(6) preparation of an offence committed with terrorist intent;
(7) an aggravated customs offence;
(8) aggravated concealment of illegally obtained goods;
(9) preparation of the taking of a hostage; or
(10) preparation of aggravated robbery.

The court decides on traffic data monitoring referred on the request of an official with the power of arrest. 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.

Content data:

Telecommunications interception refers to the monitoring, recording and other processing of a message sent to or transmitted from a network address or terminal end device through a public communications network or a communications network connected thereto, in order to determine **the contents of the message and the identifying data connected to it**.

Telecommunications interception may be directed only at a message that originates from or is intended for a suspect in an offence.

A criminal investigation authority may receive permission for telecommunications interception directed at a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect him or her of:

(1) genocide, preparation of genocide, a crime against humanity, an aggravated crime against humanity, a war crime, an aggravated war crime, torture, violation of a prohibition against chemical weapons, violation of a prohibition against biological weapons, violation against a prohibition against anti-infantry mines;
(2) endangerment of the sovereignty of Finland, incitement to war, treason, aggravated treason, espionage, aggravated espionage, disclosure of a national secret, unlawful gathering of intelligence;
(3) high treason, aggravated high treason, preparation of high treason;
(4) aggravated distribution of a sexually offensive picture depicting a child;
(5) sexual abuse of a child, aggravated sexual abuse of a child;
(6) manslaughter, murder, homicide, preparation of an aggravated offence directed against life or health as referred to in Chapter 21, section 6a of the Criminal Code and in accordance with sections 1, 2 and 3 of said Chapter;
(7) arrangement of aggravated illegal entry into the country, aggravated deprivation of liberty, trafficking in persons, aggravated trafficking in persons, kidnapping, preparation of kidnapping;
(8) aggravated robbery, preparation of aggravated robbery, aggravated extortion;
(9) aggravated concealment of illegally obtained goods, professional concealment of illegally obtained goods, aggravated money laundering;
(10) criminal mischief, criminal traffic mischief, aggravated sabotage, aggravated endangerment of health, a nuclear device offence, hijacking;
(11) an offence committed with terrorist intent, preparation of an offence committed with terrorist intent, directing of a terrorist group, promotion of the activity of a terrorist group, provision of training for the commission of a terrorist offence, recruitment for the commission of a terrorist offence, financing of terrorism, as referred to in Chapter 34(a), section 1, subsection 1, paragraphs 2-7 or subsection 2 of the Criminal Code;
(12) aggravated damage to property;
(13) aggravated fraud, aggravated usury;
(14) aggravated counterfeiting;

(15) aggravated impairment of the environment; or
(16) an aggravated narcotics offence.

A warrant for telecommunications interception may be issued also when there are grounds to suspect a person of the following in connection with commercial or professional activity:

(1) aggravated giving of a bribe;
(2) aggravated embezzlement;
(3) aggravated tax fraud, aggravated assistance fraud;
(4) aggravated forgery;
(5) aggravated dishonesty by a debtor, aggravated dishonesty by a debtor;
(6) aggravated taking of a bribe, aggravated abuse of public office;
(7) aggravated regulation offence;
(8) aggravated abuse of insider information, aggravated market price distortion; or
(9) an aggravated customs offence

The court decides on telecommunications interception on the request of an official with the power of arrest.

The warrant for telecommunications interception may be given for at most one month at a time.

8. Voluntary-disclosure:

a. **As issuing state: Admissibility of the electronic evidence obtained by voluntary disclosure.**

Evidence obtained by voluntary disclosure is used the same way as if it was obtained through regulated international cooperation.

b. As executing state: Procedures/legislation in your Member State with regards to the possibility for the OSPs in your Member State to provide data directly to other Member States

This is not possible at the moment in Finland.

9. Data retention periods (including procedures for extensions)

A data retention order is issued for ***three months at a time***.

The order may be renewed when required by the investigation of the offence. The order shall be rescinded as soon as it is no longer necessary.

10. Procedure for data preservation/execution deadline

If there are reasons to assume that data, that may be of significance for the clarification of the offence, is deleted or is changed, an official with the power of arrest may issue a data retention order.

Such an order requires that a person holding or administering data maintain the data unchanged.

The order may apply also to data that can be assumed to be transmitted to a device or information system within the month following the issuing of the order. On request, a written certificate shall be given of the order, detailing the data that is the object of the order.

11. Procedure for data production/ execution deadline

Data is finally produced through above mentioned requests to service providers or by using aforementioned coercive measures.

12. Concise legal practical information

Law enforcement authorities can obtain any kind of evidence by using different coercive measures possible by law or by requests to service providers – including evidence in the form of electronic data. Law enforcement authorities can under national law: make a request for information to service providers, confiscate/copy a document, make a search of data contained in a device/remote search and request a warrant for a traffic data monitoring or for a telecommunications interception. National competent authority to receive and execute request is the National Bureau of Investigation of Finland.

The Communication Centre handles all incoming requests 24/7 – the Communication Centre is also the SPOC for the Budapest Convention. Siena- and Interpol channels are also used. All urgent request should be pointed to the Communication Centre via Interpol, Siena and SIRENE channels.

Main instruments used are EIO, Budapest Convention and applicable bilateral treaties.

Acceptable languages are Finnish, Swedish and English.

Information related to data categories, requirements and thresholds for access please see answers in question 7.

Data retention: a data retention order is issued for three months at a time.