Fiches Belges on electronic evidence

Latvia

1. Definition of electronic evidence

Criminal Procedure Law
Section 136. Electronic Evidence

Evidence in criminal proceedings may be information regarding facts in the form of electronic information that has been processed, stored, or broadcast with automated data processing devices or systems.

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

All measures that are possible in the national criminal proceedings, are also possible in the international cooperation, including those mentioned in the Budapest Convention (however, according to Article 29, paragraph 4, dual criminality is required).

Apart from that, the Criminal Procedure Law allows to perform the following measures:

1. search and seizure (Section 179);
2. withdrawal (for example, when search and seizure is not necessary since evidence is located in publicly accessible place - Section 186);
3. submission of objects and documents on the basis of the instigative of a person (for example, when owner/handler of an object submits it on a voluntary basis - Section 189);
4. submission of objects and documents requested by the person directing the proceedings (for example, without performing search or withdrawal, investigator/prosecutor has the right to request the evidence from owner/handler. In case if they refuse to submit evidence on a voluntary basis, search or seizure, or withdrawal should be performed - Section 190);
5. storage (preservation) of data located in an electronic information system (hereinafter – EIS, Section 191);
6. disclosure and issue (submission) of data stored in an electronic information system (Section 192);
7. control of means of communications (for example, interception of phone calls or other means of communication - Section 218);
8. control of data located in an automated data system (i.e., access, search and seizure of data without informing owner/possessor of the system - Section 219);
9. control (interception) of the content of transmitted data (Section 220).

3. Procedure for obtaining electronic evidence

a. National procedures

The national procedures are provided for in the Criminal Procedure Law. However, with regard to obtaining electronic evidence, the rules of the Electronic Communications Law apply. The officials competent to perform and authorise measures depend on the severity of crime and on the level of intrusion into privacy. In case when the authorisation of an investigative judge is needed (for example, to perform a search), the person directing the proceedings (investigator or prosecutor) must present a motivated application why this measure is needed for investigation.

In short, competent authorities and rules for the measures are the following:

1. **search and seizure** is performed on the basis of the decision of an investigative judge which is taken upon an application of an investigator/prosecutor. In urgent cases search may be performed with the consent of a prosecutor, however, the documents related to search and its result must be presented to the judge within one working day. Judge then examines the validity and validity of the search;
2. **withdrawal** is performed upon a decision taken by investigator/prosecutor;
3. **submission of objects and documents** – a person that owns/handles objects or documents with the evidentiary value has the right to submit them on a voluntary basis. No decision is needed;
4. **submission of objects and documents requested by the person directing the proceedings** – a written request of investigator/prosecutor is needed. In case if a person refuses to submit the evidence, either search or withdrawal may be performed (depends on the location of evidence and procedural guarantees);
5. **preservation of data located in an electronic information system** - investigator/prosecutor may assign the owner/possessor of EIS to ensure the storage of data in an unchanged state and without accessibility of such data to other users of the system. The preservation may be assigned for 30 day, which may be prolonged for another 30 days. This rule does not apply to data, retention of which is specified by Electronic Communication Law, i.e. subscriber, traffic and location data.
6. **disclosure and issue of data stored in an electronic information system**
   The disclosure procedure depends on the basis upon which data has been preserved:
   1) for subscriber, traffic and location data (which are retained according to the Electronic Communication Law) – written request of investigator with the consent of prosecutor or data subject is needed (or – written request of prosecutor with the consent of higher-ranking prosecutor or data subject is needed - Section 192 (1) of Criminal Procedure Law);
   2) for disclosure of other data (for example, content data), which have been preserved upon a decision of investigator/prosecutor, the decision of an investigative judge is needed (or consent of data subject- Section 192 (2) of Criminal Procedure Law).
7. **control of means of communications; control of data located in an automated data system; control (interception) of the content of transmitted data –** all these measures belong to so-called special investigative measures and may be performed only upon a decision of investigative judge for a period of time up to 30 days (may be prolonged, if there is a reason). The criteria for severity of crimes applies (may not be performed for investigation of criminal violation).

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)

1. MLA/EIO procedure – the competent authorities could be found in the Judicial Atlas on the EJN Website. Depending on the measure and the stage of procedure, EIO/MLA request should be sent to:

1) in pre-trial proceedings - Prosecutor General's Office of Latvia (or State Police)
2) during the trial stage – Ministry of Justice.

The grounds for procedural assistance are the following:

1) a request of a foreign country;
2) a decision of the competent authority of Latvia on admissibility of a procedural action (i.e., that the execution of a request is possible).

2. 24/7 Network

The operational 24/7 contact point is the 1st Unit of the International Cooperation Department (Unit) of the Central Criminal Police Department of the State Police.
The Unit acts as an international criminal judicial cooperation "front office", providing a single point of contact (SPOC) by coordinating all international exchange of information in the 24/7 regime (Interpol, Europol, SIRENE, cooperation in criminal matters, cybercrime contact point). Thus, Latvia has implemented a "one stop shop" concept by including all the international police cooperation services in a common data acquisition and processing flow.

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

1. 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters and its 1978 Protocol.
2. Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union
3. Council of Europe Convention on Cybercrime, Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer
4. Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union
5. Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters

5. competent authority to receive and execute your request

MLA/EIO procedure – the competent authorities could be found in the Judicial Atlas on the EJN website. Depending on the measure and the stage of procedure, EIO/MLA request should be sent to:

1) for pre-trial proceedings - Prosecutor General's Office of Latvia (or State Police)
2) during the trial stage – Ministry of Justice.

The grounds for procedural assistance are the following:

1) a request of a foreign country;
2) a decision of the competent authority of Latvia on admissibility of a procedural action (i.e., that the execution of a request is possible).

In the pre-trial stage, depending on a measure, competent authority either executes request or assigns an authority that executes the request.

6. accepted languages

Latvian/English (for requests in English an additional time for translation is needed that may cause delay in execution).

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

The definitions of data categories are provided for in Electronic Communications Law:

1) location data - data which is processed in an electronic communications network or processed using electronic communications services and indicates the location of the terminal equipment of an electronic communications service user. For public mobile electronic communications networks, satellite networks, and non-wire networks which are used for the distribution of radio or television signals, it shall be the geographic location (address) of the terminal equipment of an electronic communications service user, but for public fixed networks, cable television, and cable radio networks, and electricity cable systems to the extent that they are used in order to transmit electronic communications signals - the termination point address;

2) traffic data - any information or data which is processed in order to transmit information by an electronic communications network or to prepare accounts and register payments, except the content of transmitted information.

3) data to be retained - the traffic data referred to [in Annexes 1 and 2 to this Law], location data and the associated data thereof, which is necessary in order to identify the subscriber or user.

In terms of severity of crime, there is no threshold for access to different data categories.

There are different rules for access to different data categories (as is mentioned above, in p.3.a) The disclosure procedure depends on the basis upon which data has been preserved:

1) **for subscriber, traffic and location data** (which are retained according to the Electronic Communication Law) – written request of investigator with the consent of prosecutor or data subject is needed (or – written request of prosecutor with the consent of higher-ranking prosecutor or data subject is needed);

2) **for disclosure of other data (for example, content data)**, which have been preserved upon a decision of investigator/prosecutor, the decision of an investigative judge is needed (or consent of data subject).

8. Voluntary-disclosure:

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

Pursuant to Criminal Procedure Law, evidence is admissible if it was obtained and procedurally fixed in accordance with the procedures laid down in this law (Section 130).

Criminal Procedure Law does not foresees the voluntary disclosure of the electronic evidence. To use it as evidence it should be obtained in the following procedure:

1) for subscriber, traffic and location data (which are retained according to the Electronic Communication Law) – written request of investigator with the consent of prosecutor or data subject is needed (or – written request of prosecutor with the consent of higher-ranking prosecutor or data subject is needed);

2) for disclosure of other data (for example, content data), which have been preserved upon a decision of investigator/prosecutor, the decision of an investigative judge is needed (or consent of data subject).

Voluntarily disclosed information may be used only for intelligence purposes.

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

No regulation in this regard. In general, the procedure laid down in the Electronic Communication Law should be respected that foresees the cooperation only between OSP and Latvian authorities.

9. Data retention periods (including procedures for extensions)

18 months for subscriber, traffic and location data (Art. 19 (1) 11); 71.1 of the Electronic Communications Law).

10. Procedure for data preservation/execution deadline

30 days (may be extended for another 30 day, does not apply to data that are to be retained pursuant to Electronic Communications Law). The decision of investigator/prosecutor is needed (Section 191, Criminal Procedure Law).

11. Procedure for data production/ execution deadline

The disclosure procedure depends on the basis upon which data has been preserved:

1) **for subscriber, traffic and location data** (which are retained according to the Electronic Communication Law) – written request of investigator with the consent of prosecutor or data subject is needed (or – written request of prosecutor with the consent of higher-ranking prosecutor or data subject is needed; in the trial stage – request from a judge/court - Section 192 (1) of Criminal Procedure Law);
2) **for disclosure of other data (for example, content data)**, which have been preserved upon a decision of investigator/prosecutor, the decision of an investigative judge is needed (or consent of data subject – Section 192 (2) of Criminal Procedure Law).

12. Concise legal practical information