EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

Lithuania

1. **Definition of electronic evidence**

Lithuania has no legal definition of electronic evidence.

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

All of the measures provided in the third chapter of the 2001 Budapest Cybercrime Convention are possible:

a. *Spontaneous information (Art. 26 Budapest Convention)*
b. *Expedited preservation (Art. 29 Budapest Convention)*
c. *Expedited disclosure of traffic data (Art. 30 Budapest Convention)*
d. *Production orders/access to data (Art. 31 Budapest Convention)*
e. *Spontaneous information (Art. 26 Budapest Convention)*
f. *Trans-border access to stored computer data with consent or where publicly available (Art. 32 Budapest Convention)*
g. *real-time collection of traffic data (Art. 33 Budapest Convention)*
h. *interception of content data (Art. 34 Budapest Convention)*

In relation to EU Member States Lithuania applies the Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO) and its implementing legislation.

In relation to other states it is possible to grant mutual legal assistance as provided for in the European Convention on Mutual Legal Assistance in Criminal Matters (including its protocols) and several other bilateral and multilateral agreements on MLA.

3. **Procedure for obtaining electronic evidence**

a. National procedures

National legal framework for obtaining stored data (e-evidence) from service providers is set out in the Criminal Procedure Code, Law on Electronic Communications and Law on Cyber Security.

The main rule for obtaining e.evidence from service providers is Article 155 of the Criminal Procedure Code. According to this Article, a prosecutor has to take a decision and obtain the consent of a pre-trial investigation judge to issue the production order. In addition, a pre-trial investigation officer may, on the assignment of a prosecutor, access information in accordance with the procedure stipulated in this Article.

According to the Article 160[1] of the Criminal Procedure Code in urgent cases, order could be issued by prosecutor. In this case, an order of a pre-trial investigation judge approving the legitimacy of the order must be obtained within three days from the taking of the decision.

According to General Prosecutor order No. I-383 of December 31, 2012[1], the prosecutor's decision and the investigation judge consent shall not be required to obtain information directly related to telephone numbers or electronic communications terminal equipment, telephone number, email address or network terminal equipment dependency, or to natural or legal person account numbers or bank accounts or dependence of financial and / or payment instruments and persons entitled to dispose of it.

---

1 https://www.e-tar.lt/portal/lt/legalAct/TAR.FB0E47A36ED6

According to the Article 10 of Law on Cyber Security the Police has the right to issue an order to the provider of public communications networks and or public digital communications service provider, digital information hosting service provider and digital service provider to preserve and get information related to the services provided by them which might help detect the type of communications service used, technical measures which were applied and the times of usage, identify the recipient of services, mail address, geographical location address, phone or any other access number, information about accounts and payments made on the basis of service agreement and other information which is available in the location where communications equipment is installed, on the basis of the existing service contract or agreement, and with the court ruling substantiated available, to receive the data of service recipients' flow.

Law on Electronic Communications regulates social relations pertaining to electronic communications services and networks, associated facilities and services, use of electronic communications resources as well as social relations pertaining to radio equipment, terminal equipment and electromagnetic compatibility. The Law determines the duties of Undertakings providing electronic communications networks to keep and without payment provide to the competent institutions data generated or processed by them as specified in paragraph 1 of the Annex to this Law.

Regarding to the real-time interception in criminal proceedings, the main provisions for real-time interception are established in the Article 154 of the Criminal Procedure Code. According to this Article a prosecutor has to obtain the consent of a pre-trial investigation judge to issue the order. Grounds to issue the order: there is a ground for believing that in this manner, data could be obtained on a grave, serious or less serious crime being planned, being or having been committed or on minor crimes provided for in Article 152-1, Article 162(2), Article 170, Article 198-2(1) and Article 309(2) of the Criminal Code of the Republic of Lithuania or where there is a risk that the victim, a witness or other participants in the proceedings or close persons thereof may be exposed to violence, coercion or other unlawful acts. This procedure may be applied to control and documenting of the information transmitted by electronic communications networks, with the exception of the content thereof, where there is a ground for believing that in this manner, data could be obtained on the minor crimes provided for in Articles 166 and 198-1 and Article 309(1) of the Criminal Code of the Republic of Lithuania

Please find below the relevant provisions for these legal acts.

CRIMINAL PROCEDURE CODE OF THE REPUBLIC OF LITHUANIA

"Article 154. Control, documenting and accumulation of information transmitted by electronic communications networks

1. Upon issuing an order of a pre-trial investigation judge at the request of a prosecutor, a pre-trial investigation officer may wiretap personal conversations transmitted by electronic communications networks, make recordings thereof, control, document and accumulate other information transmitted by electronic communications networks where there is a ground for believing that in this manner, data could be obtained on a grave, serious or less serious crime being planned, being or having been committed or on minor crimes provided for in Article 152-1, Article 162(2), Article 170, Article 198-2(1) and Article 309(2) of the Criminal Code of the Republic of Lithuania or where there is a risk that the victim, a witness or other participants in the proceedings or close persons thereof may be exposed to violence, coercion or other unlawful acts.

2. In an order of a pre-trial investigation judge or a decision of a prosecutor to wiretap personal conversations transmitted by electronic communications networks, to make recordings thereof, to control other information transmitted by electronic communications networks and to document and accumulate it, the following must be indicated:

1) the available data on the person against whom the actions must be carried out;

2) the data justifying the necessity to carry out the actions provided for in paragraph 1 of this Article;

3) the specific actions provided for in paragraph 1 of this Article the carrying out whereof is authorised;

4) the duration of the carrying out of the actions.

3. The procedure laid down in paragraph 1 of this Article may apply to control and documenting of the information transmitted by electronic communications networks, with the exception of the content thereof, where there is a ground for believing that in this manner, data could be obtained on the minor crimes provided for in Articles 166 and 198-1 and Article 309(1) of the Criminal Code of the Republic of Lithuania.

4. The duration of wiretapping of personal conversations transmitted by electronic communications networks, making records thereof or controlling, documenting and accumulation of other information transmitted by electronic communications networks may not exceed six months. When investigating a complicated or large-scale criminal act, application of this measure may be extended once for a period of three months.

5. The economic entities providing electronic communications networks and/or services must provide conditions for wiretapping of personal conversations transmitted by electronic communications networks, making records thereof or controlling, documenting and accumulating other information transmitted by electronic communications networks. The employees of an economic entity providing electronic communications networks and/or services who fail to comply with this obligation or interfering with the actions referred to in this Article may be subject to a fine in compliance with Article 163 of this Code.

6. Conversations of victims, witnesses or other participants in proceedings transmitted by electronic communications networks may be wiretapped, recordings may be made thereof, other information transmitted by these persons by electronic communications networks may be controlled, documented and accumulated at the request of these persons or subject to their consent also in the absence of an order of a pre-trial investigation judge issued thereon, unless the services and facilities of the economic entities providing electronic communications networks and/or services are accessed.

7. It shall be prohibited to wiretap the conversations of the defence counsel with the suspect or the accused transmitted by electronic communications networks, make recordings thereof, control other information transmitted between them by electronic communications networks, document and accumulate it.

8. As regards the fact of control of the content of conversations transmitted by electronic communications networks or other information transmitted by electronic communications networks, a record drawn up by a pre-trial investigation officer shall contain solely the data and audio content relevant to the investigation. The data and audio recordings not relevant to the investigation and not kept in a medium together with the data and recordings relevant to the case shall not be attached to the case file and shall be immediately destroyed by a decision of a prosecutor upon drawing up a relevant note."

"Article 155. Prosecutor's right to access information

1. A prosecutor who has taken a decision and has obtained the consent of a pre-trial investigation judge shall have the right to come to any state or municipal, public or private agency, undertaking or organisation and to request to be provided with access to the required documents or other required information, to make recordings or to copy documents and information or to obtain the indicated information in writing, if it is necessary for the investigation of a criminal act.

2. The persons who refuse to provide the required information or documents to a prosecutor may, pursuant to Article 163 of this Code, be imposed a fine.

3. A prosecutor may use the information obtained in accordance with the procedure laid down in paragraph 1 of this Article only for the investigation of a criminal act. The prosecutor must immediately destroy the information that is not necessary for the investigation of the criminal act.

4. A pre-trial investigation officer may, on the assignment of a prosecutor, also access information in accordance with the procedure stipulated in this Article.

5. Laws of the Republic of Lithuania may stipulate restrictions regarding the prosecutor's right of access to information."

"Article 160[1]. Use of procedural coercive measures in urgent cases

1. In urgent cases, the procedural coercive measures provided for in Articles 154, 155, 158 and 159 of this Code may also be applied by a decision of a prosecutor and the procedural coercive measures provided for in Articles 145, 147 and 160 of this Code - also by a decision of the prosecutor or a pre-trial investigation officer, but in all these cases an order of a pre-trial investigation judge approving the legitimacy of the application of a procedural measure must be obtained within three days from the taking of the decision. This order of the pre-trial investigation judge shall be appealed against in accordance with the procedure laid down in Part X of this Code. The filing of an appeal against the order of the pre-trial investigation judge refusing to approve the legitimacy of the application of the procedural coercive measure shall suspend the enforcement of this order.

2. If an order of a pre-trial investigation judge is not issued within the time limit laid down in paragraph 1 of this Article, the actions initiated by a decision of a prosecutor or a pre-trial investigation officer shall be terminated without delay.

3. If an order approving the legitimacy of the application of a procedural coercive measure is not received, the items, valuables and documents seized during a search or a seizure shall be returned to the persons from whom they were seized and the data received by means of other procedural coercive measures shall be destroyed. This shall be done after the expiry of a time limit specified in paragraph 1 of this Article or a time limit for appealing against an order of a pre-trial investigation judge or, when this order has been appealed against, upon taking a decision by a higher court. In these cases, the results of the application of the procedural coercive measures may not be relied upon in further proceedings as the data evidencing the guilt of the suspect or the accused."

"Article 161. Notification to a person of the measures applied against him

1. A person who, without his knowledge, has been subject to at least one of the measures provided for in this Chapter must be notified thereof upon completion of the application of such a measure. It shall be necessary to notify the person as soon as this becomes possible without compromising the success of the investigation.

2. If criminal proceedings are terminated, all the information collected about the private life of a person must be destroyed without delay upon drawing up a relevant note. A decision on the destruction of such information shall be taken by a prosecutor after the expiry of a time limit for appealing against a procedural decision to terminate a pre-trial investigation as provided for in Article 214 of this Code or after examining appeals of the participants in the proceedings regarding the termination of the pre-trial investigation.

3. Certain information must also be destroyed in accordance with the procedure provided for in paragraph 2 of this Article if it is decided that such information or its part will not be used in criminal proceedings as having no relation thereto, even though the criminal proceedings are not terminated."

"Article 162. Use of information in other criminal cases

The information collected in one criminal case about the private life of a person using the procedural coercive measures provided for by this Code may be used during a pre-trial investigation in another criminal case only by a decision of a senior prosecutor. If the criminal case is being heard by a court, a decision on the use of the information in another criminal case shall be taken by an order of a pre-trial investigation judge or the court."

"Article 163. Coercive measures applicable against the persons failing to comply with lawful instructions of a pre-trial investigation officer, a prosecutor, a pre-trial investigation judge or a court

1. A witness who, without a valid reason, fails to appear for participate in proceedings or any person who fails to comply with the lawful instructions of a pre-trial investigation officer, a prosecutor, a pre-trial investigation judge or a court issued in accordance with this Code or other laws or who interferes with the investigation of a criminal case may be subject to a fine in the amount of up to thirty minimum standards of living (MSLs) and, in the cases provided for in this Code, arrest for a period of up to one month. The fine may be imposed by a prosecutor, the pre-trial investigation judge or the court, and arrest - only by the pre-trial investigation judge or the court. The suspect or the accused may be subject to the fine specified in this Article only for a failure to participate in proceedings without a valid reason.

2. A prosecutor shall impose a fine by a decision of his own motion or on the basis of a statement made by a pre-trial investigation officer. A pre-trial investigation judge or a court shall impose the fine or arrest of its own motion or at the request of the prosecutor.

3. A decision of a prosecutor to impose a fine may be appealed against in accordance with the procedure stipulated in Article 63 of this Code within ten days from the receipt of a transcript thereof.

4. A person subject to a fine or arrest may appeal against an order of a pre-trial investigation judge or a court hearing the case to impose a fine or arrest within seven days from the receipt of a transcript of the order to the pre-trial investigation judge or the court that has issued the order requesting to revoke the imposed fine or arrest or to reduce the amount of the fine or the duration of arrest. The appeal shall be examined at a court sitting if a notice thereof has been given to the person who has filed the appeal. An order issued in respect of the appeal may be appealed against to a higher court in accordance with the procedure laid down in Part X of this Code."

LAW ON ELECTRONIC COMMUNICATIONS OF THE REPUBLIC OF LITHUANIA

"Article 34. Duties and rights of public electronic communications service providers and end users

(…)

14. Undertakings providing electronic communications networks and/or services shall designate natural persons to work with communications of entities of criminal intelligence and intelligence institutions, use of technical measures in their networks in accordance with special procedure, be responsible for fulfilment of enquiry requirements of entities of criminal intelligence, pre-trial investigation institutions, prosecutors, courts or judges. Such natural persons must have security clearance and must be authorised to work with or have access to classified information in accordance with the procedure established by the Government.

(…)"

"Article 65. Data categories

(…)

2. In order to ensure that data are available for the purposes of investigation, detection and prosecution of criminal offences of serious and particularly serious crimes[2], as defined by the Criminal

---

2 According to the Criminal Code premeditated crimes are divided into minor, less serious, serious and grave crimes. A minor crime is a premeditated crime punishable, under the criminal law, by a custodial sentence of the maximum duration of three years. A less serious crime is a premeditated crime punishable, under the criminal law, by a custodial sentence of the maximum duration in excess of three years, but not exceeding six years of imprisonment. A serious crime is a premeditated crime punishable, under the criminal law, by a custodial sentence

Code of the Republic of Lithuania, providers of public communications networks and/or public electronic communications services must keep and without payment provide to the competent institutions data generated or processed by them as specified in paragraph 1 of the Annex to this Law."

"Article 66. Data processing

(…)

6. Data referred to in Article 65(2) of this Law, except for the data specified in paragraph 6.3 of Annex 1 of this Law, shall be stored for six months from the date of the communication. Data referred to paragraph 6.3 of Annex 1 of this Law shall be stored for two months from the date of the communication."

"Article 77. Supervision and monitoring of electronic communications traffic

(…)

3. If the data referred to in Article 65 of this Law are necessary for entities of criminal intelligence, intelligence institutions, pre-trial investigation institutions, prosecutors, courts or judges to prevent, investigate and detect criminal acts, upon the instruction of the institutions authorised by the Government, i.e. an entity of criminal intelligence or an intelligence institution, the undertakings providing electronic communications networks and/or services must extend the retention period of this information specified in paragraphs 4, 5 and 6 of Article 66 of this Law, except for the data specified in paragraph 6.3 of Annex 1 of this Law, but by no longer than six months. Such storage shall be paid for with state budget funds in accordance with the procedure established by the Government.

Annex 1 to
Republic of Lithuania
Law on Electronic Communications

"DATA CATEGORIES TO BE PROTECTED

1. Data necessary to trace and identify the communication source:

1.1. related to fixed telephone communications network and mobile telephone communication:

1.1.1. telephone number from which the call is made;

1.1.2. name and surname (name) and address of the subscriber or registered user of electronic communications services;

1.2. related to Internet access, Internet e -mail and Internet telephony:

1.2.1. user identification codes issued;

1.2.2. user identification codes and telephone numbers issued to all communications via public telephone network;

1.2.3. identification code, telephone number, name and surname (name) and address of the subscriber or registered user of electronic communications services, which was assigned an Internet Protocol (IP) address.

2. Data necessary to identify the communication destination:

---

of the duration in excess of three years, but not exceeding ten years of imprisonment. A grave crime is a premeditated crime punishable, under the criminal law, by a custodial sentence of the maximum duration in excess of ten years.

2.1. related to fixed telephone communications network and mobile telephone communication:

2.1.1. telephone number or numbers dialled (telephone number to which the call is made), and additional services, such as, for example, in call forwarding or call transfer cases, telephone number or numbers to which the call is routed;

2.1.2. the name and surname (name) and address of the subscriber or registered user of electronic communications services;

2.2. related to the Internet e-mail and Internet telephony:

2.2.1. identification code or telephone number of the intended telephone call by Internet user/users;

2.2.2. the name and address of the subscriber or registered user of electronic communications services and identification code of the intended telephone call by the Internet user.

3. Data necessary to identify the date, time and duration of a communication:

3.1. related to fixed telephone communications network and mobile telephone communication, i.e. communication date and the beginning and end of time of the communication or the beginning time and duration of communication;

3.2. related to Internet access, Internet e-mail and Internet telephony:

3.2.1. date and time in a particular time zone of the connection to and log off the Internet access service, dynamic or static Internet Protocol (IP) address, which was issued by the provider of Internet access service, and the identification code of the subscriber or registered user of electronic communication services;

3.2.2. date and time in a particular time zone of the connection to and log off the Internet e-mail service or Internet telephony service.

4. Data necessary to identify the type of communication:

4.1. related to the fixed telephone network and mobile telephone network, i.e. the telephone network service that is used;

4.2. relating to Internet access, Internet e-mail and Internet telephony, i.e. the Internet service that is used.

5. Data necessary to identify users' communication equipment or what purports to be their equipment:

5.1. related to fixed telephone network, i.e. telephone numbers to which and from which the call is made;

5.2. associated with mobile telephone connection:

5.2.1. telephone numbers to which and from which the call is made;

5.2.2. the International Mobile Subscriber Identity (IMSI) of the calling country;

5.2.3. the International Mobile Equipment Identity (IMEI) of the calling country;

5.2.4. the International Mobile Subscriber Identity (IMSI) of the called country;

5.2.5. the International Mobile Equipment Identity (IMEI) of the called country;

5.2.6. in case of Mobile Equipment pre-paid service, the initial activation in the Republic of Lithuania date, time and label of location, where the service has been activated (Cell ID);

5.3. related to Internet access, Internet e -mail and Internet telephony:

5.3.1. calling phone number used for dial-up connections;

5.3.2 . digital subscriber line (DSL) or other end points of the originator of a message .

6. The data required to identify the location of mobile communications equipment:

6.1. location label (Cell ID) at the beginning of communication;

6.2. data necessary to determine the geographical location of network equipment corresponding to the location label (Cell ID) at a moment of time when communications data are saved.

6.3. data required to identify the geographic location of network equipment that corresponds to a Location Tag Area (LAI) as defined by telecommunications standards;

6.4. data on the active (used) base stations coverages cells of the undertaking providing the mobile communication services:

6.4.1. Location Tag (Cell ID)
6.4.2. geographical coordinates;
6.4.3. direction of the signal being transmitted during the request."

"Article 77. Supervision and monitoring of electronic communications traffic

1. Main institutions of criminal intelligence services, pre-trial investigation institutions, prosecutors, courts or judges must be provided in accordance with the procedure established by the law by undertakings providing electronic communications networks and/or services with the information which is available to them and which is necessary to prevent, investigate, and detect criminal acts. Undertakings providing electronic communications networks and/or services, must provide entities of criminal intelligence in accordance with the procedure established by the law with information necessary for forecasting, identifying or eliminating risks that may have significance for the national sovereignty, territorial integrity and inviolability, constitutional structure, interests, defence or economic power of the state. Main institutions of criminal intelligence services and pre-trial investigation institutions designated by the Government shall be provided with the above mentioned information by undertakings providing electronic communications networks and/or services immediately, free of charge and in electronic form in response to the enquiries of the said institutions. Pre-trial investigation institutions designated by the Government shall provide their subdivisions and/or other pre-trial investigation institutions with access to such information in accordance with the procedure established by the Government. All persons taking part in the exchange of information shall make necessary arrangements to ensure data security in accordance with the procedure and under the conditions set forth by the Government; the additional equipment necessary for this purpose shall be obtained from and maintained with Government funds. If the information presented by an undertaking providing electronic communications networks and/or services needs to be confirmed for pre-trial investigation purposes, the pre-trial investigation officer shall directly address the undertaking in writing and the undertaking shall provide a written response.

2. Undertakings providing electronic communications networks and/or services shall, in implementing the provisions of paragraph 1 of this Article, approve internal rules for the management of requests and/or enquiries for providing the information. Undertakings providing electronic communications networks and/or services shall provide information, at the request of the State Data Protection Inspectorate, about these procedures, the number of applications and/or enquiries, their legal basis and the answers provided.

3. If the data referred to in Article 65 of this Law are necessary for entities of criminal intelligence, intelligence institutions, pre-trial investigation institutions, prosecutors, courts or judges to prevent, investigate and detect criminal acts, upon the instruction of the institutions authorised by the Government, i.e. an entity of criminal intelligence or an intelligence institution, the undertakings providing electronic communications networks and/or services must extend the retention period of this information (except data specified in paragraph 6.3. of the Annex to this Law) specified in paragraphs 4, 5 and 6 of Article 66 of this Law, but by no longer than six months. Such storage shall be paid for with state budget funds in accordance with the procedure established by the Government.

(…)"

LAW ON CYBER SECURITY OF THE REPUBLIC OF LITHUANIA

"Article 10. Powers of the Police in the field of cyber security

When implementing the prevention of cyber incidents which possibly have constituent elements of criminal offences and when conducting their investigation, the Police:

(…)

4) has the right to issue an order to the provider of public communications networks and or public digital communications service provider, digital information hosting service provider and digital service provider to preserve information related to the services provided by them which might help detect the type of communications service used, technical measures which were applied and the times of usage, identify the recipient of services, mail address, geographical location address, phone or any other access number, information about accounts and payments made on the basis of service agreement and other information which is available in the location where communications equipment is installed, on the basis of the existing service contract or agreement, get this information, and with the court ruling substantiated available, to receive the data of service recipients' flow and control the content of transferred information specified herein."

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)

There is no specific domestic framework for MLA according to the Budapest Convention.

Requests for data preservation and partial disclosure of traffic data as set out in Articles 16 and 17 of the Budapest Convention are to be submitted to 24/7 point of contact established within the Lithuanian Police. As a general rule, foreign law enforcement agencies also use liaison officers and other police-to-police cooperation channels, such as Europol or Interpol secure communication channels, to pass these requests.

For full disclosure of preserved electronic evidence, regular EIO and MLA procedures and channels are used, including EUROJUST and EJN.

As a general rule, requests to obtain electronic evidence in criminal matters (EIO and MLA) are submitted via judicial networks (such as EUROJUST and European Judicial Network). Alternatively, requests are submitted through other channels, including police-to-police cooperation channels (Budapest Convention 24/7 point of contact established within the Lithuanian Police, INTERPOL, EUROPOL), liaison officers, as well as through direct communication between competent institutions of the requesting and requested states by phone, email or fax, including advance contact of foreign authorities to alert them of impending request. These channels are also used for urgent cases.

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

In relation to EU Member States, Lithuania applies the Directive 2014/41/EU regarding the European Investigation Order in criminal matters (EIO) and its implementing legislation; Convention on Mutual Assistance in Criminal Matters between the Members States of the European Union. Also, relevant provisions of Budapest Convention regarding data preservation are applicable to EU Member States.

In relation to other states: the Budapest Cybercrime Convention, the European Convention on Mutual Legal Assistance in Criminal Matters (including its protocols) and several other bilateral and multilateral agreements on MLA.

5. Competent authority to receive and execute your request

Regarding the European Investigation Order (Directive 2014/41/EU):

The issuing authorities in Lithuania are the following judicial authorities:

- during court proceedings, the court hearing the case;

- during pre-trial investigations, the regional prosecutor's office, if a European Investigation Order is issued while the regional prosecutor's office is conducting a pre-trial investigation or on receipt of a request from a pre-trial investigation body whose pre-trial investigations are being led by the regional prosecutor's office;

- the Prosecutor General's Office, if a European Investigation Order is issued while the Prosecutor General's Office is conducting a pre-trial investigation or on receipt of a request from a pre-trial investigation body whose pre-trial investigation is being led by the Prosecutor General's Office, or on receipt of a request from the prosecutor or court leading the pre-trial investigation if it is necessary to transfer temporarily to or from Lithuania a person held in custody or a person serving a sentence involving deprivation of liberty.

The executing authorities in Lithuania are as follows:

- the district court, where the European Investigation Order is issued during court proceedings;

- the regional prosecutor's office, where the European Investigation Order is issued during a pre-trial investigation;

- the Prosecutor General:

1) where it is necessary, in accordance with Article 22 or 23 of the Directive, to transfer temporarily to or from Lithuania a person held in custody or a person serving a sentence involving deprivation of liberty;

2) where the European Investigation Order is issued during a pre-trial investigation, and;

a) it is not possible to establish the specific territory in Lithuania where the European Investigation Order is to be enforced, or

b) there are several territories in which the European Investigation Order is to be enforced and coordination of the enforcement is required.

The designated central authorities that are required to provide assistance to the competent authorities are the Ministry of Justice at the stage of court proceedings and the Prosecutor General's Office at the stage of the pre-trial investigation.

The body competent to receive notifications referred to in Article 31 of the Directive (notification of the Member State where the subject of the interception is located from which no technical assistance is needed) is the Police Department under the Ministry of the Interior

Regarding the Budapest Convention on Cybercrime :

The Ministry of Justice and the General Prosecutor's Office of the Republic of Lithuania are designated as responsible authorities to perform the functions mentioned in Article 24, paragraph 7, sub-paragraph a, and Article 27.

The Police Department under the Ministry of the Interior of the Republic of Lithuania is designated as a competent authority to perform the functions mentioned in Article 35.

General rules are set out in Criminal procedure Code:

CRIMINAL PROCEDURE CODE OF THE REPUBLIC OF LITHUANIA

"Article 66. Procedure for communication of the courts and the prosecutor's office of the Republic of Lithuania with bodies of foreign states and international organisations

1. The procedure for communication of the courts and the prosecutor's office of the Republic of Lithuania with bodies of foreign states and international organisations, also the procedure for executing of requests of these bodies and organisations shall be laid down by this Code and international treaties of the Republic of Lithuania.

2. The courts and the prosecutor's office of the Republic of Lithuania shall send requests to bodies of foreign states and international organisations via the Ministry of Justice of the Republic of

Lithuania or the Prosecutor General's Office of the Republic of Lithuania. In urgent cases, requests of the courts and the prosecutor's office of the Republic of Lithuania to other Member States of the European Union may be sent via a prosecutor of the Prosecutor General's Office of the Republic of Lithuania who is National Member for Lithuania at Eurojust/Deputy National Member for Lithuania at Eurojust. In the cases provided for in international treaties of the Republic of Lithuania, the courts, the prosecutor's office and pre-trial investigation bodies of the Republic of Lithuania may send requests directly to bodies of foreign states and international organisations.

3. In the cases and in accordance with the procedure established by the Law of the Republic of Lithuania on Mutual Recognition and Execution of Decisions of the Member States of the European Union in Criminal Matters, the procedural documents aimed at collecting evidence or obtaining the evidence already collected or temporarily protecting the items, documents or another property that could be confiscated or recognised as having evidential value in criminal proceedings against destruction, replacement, removal from another Member State of the European Union, sale or other transfer may be transferred for execution to another Member State of the European Union. "

"Article 67. Execution of requests of bodies of foreign states and international organisations regarding the carrying out of procedural actions

1. The courts, the prosecutor's office or pre-trial investigation bodies of the Republic of Lithuania shall, in executing requests of bodies of foreign states and international organisations, carry out the procedural actions specified in this Code. In executing the requests of the bodies of foreign states and the international organisations, the procedural actions which are not provided for in this Code may also be carried out in the cases provided for in an international treaty of the Republic of Lithuania, provided that the carrying out of such actions does not violate the Constitution and laws of the Republic of Lithuania and is not in contradiction with the basic principles of criminal procedure in the Republic of Lithuania.

2. The courts, the prosecutor's office and pre-trial investigation bodies of the Republic of Lithuania shall receive requests of bodies of foreign states and international organisations via the Ministry of Justice of the Republic of Lithuania, the Prosecutor General's Office of the Republic of Lithuania or a prosecutor of the Prosecutor General's Office of the Republic of Lithuania who is National Member for Lithuania at Eurojust/Deputy National Member for Lithuania at Eurojust. A court, prosecutor's office or pre-trial investigation body of the Republic of Lithuania shall execute a request directly received from a body of a foreign state or an international organisation only upon obtaining a permission of the Ministry of Justice of the Republic of Lithuania or the Prosecutor General's Office of the Republic of Lithuania, with the exception of the cases indicated in paragraph 5 of this Article.

3. A request of a body of a foreign state and an international organisation which cannot be executed shall be returned to that body or organisation via the Ministry of Justice of the Republic of Lithuania, the Prosecutor General's Office of the Republic of Lithuania or a prosecutor of the Prosecutor General's Office of the Republic of Lithuania who is National Member for Lithuania at Eurojust/Deputy National Member for Lithuania at Eurojust and reasons for the non-execution of the request shall be indicated.

4. Officials of the courts, the prosecutor's office and pre-trial investigation bodies of foreign states or the International Criminal Court or other international organisations shall be allowed to carry out procedural actions in the Republic of Lithuania only in the cases provided for in an international treaty of the Republic of Lithuania and in the presence of officials of the Republic of Lithuania.

5. In the cases provided for in an international treaty of the Republic of Lithuania, the courts, the prosecutor's office and pre-trial investigation bodies of the Republic of Lithuania shall execute the requests directly received from bodies of foreign states and international organisations and send replies to the requests directly to the foreign states and to the international organisations.

6. In the cases and in accordance with the procedure established by the Law of the Republic of Lithuania on Mutual Recognition and Execution of Decisions of the Member States of the European Union in Criminal Matters, the procedural documents of another Member State of the European Union

aimed at collecting evidence or obtaining the evidence already collected or temporarily protecting the items, documents or another property that could be confiscated or recognised as having evidential value in criminal proceedings against destruction, replacement, removal from another Member State of the European Union, sale or other transfer may be executed. "

6. **Accepted languages**

Regarding the European Investigation Order (Directive 2014/41/EU): Lithuanian or English.
Data preservation requests in the framework of Budapest Convention: English.
Other MLA requests: Lithuanian.

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**

Definitions of subscriber, traffic/transaction and content data in Lithuania correspond those established in the Budapest Convention.

Subscriber data requires the lowest threshold for access. It can be requested on the basis of an official request issued by the police or a prosecutor.

Traffic and content data require higher authorization. It can be obtained on the basis of an order issued by a prosecutor and authorized by a pre-trial judge.

Real-time interception requires judicial authorization.

8. **Voluntary-disclosure:**

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

Admissible - the electronic evidence obtained by voluntary disclosure is used the same way as it was obtained through regulated international cooperation. Lithuanian legislation does not prohibit Lithuanian competent authorities to address orders and other types of requests to service providers outside the territory of Lithuania.

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 Lithuania. Currently, there are no legal measures that allow service providers under ours jurisdiction to respond to direct requests from law enforcement authorities from third countries. The only possible way to do that is to send an MLA to a respective country.

9. **Data retention periods (including procedures for extensions)**

Electronic communications service providers are bound by law to retain stored data for the period of 6 month. Data categories to be retained are specified in paragraph 1 of the Annex to the Law on Electronic Communications (see the answer to question 3). This retention period could be extended no longer than by additional six months.

10. **Procedure for data preservation/execution deadline**

Data preservation requests from another Party are handled by Budapest Convention 24/7 SPoC established within the Lithuanian Police. Upon receipt of a data preservation request, SPoC checks

and verifies both the sender and the information provided in the request to make sure legal and organizational details are intact. Following that, SPoC sends out a domestic request to a relevant online service provider (OSP) to preserve the data. Requests are processed without undue delay.

Also please see the information provided for the question 3.

11. Procedure for data production/ execution deadline

National legal framework for obtaining stored data (e-evidence) from service providers is set out in the Criminal Procedure Code, Law on Electronic Communications and Law on Cyber security. The main rule for obtaining e.evidence form service providers is the Article 155 of the Criminal Procedure Code. According to this Article, a prosecutor has to take a decision and obtain the consent of a pre-trial investigation judge to issue the production order. In addition, a pre-trial investigation officer may, on the assignment of a prosecutor, access information in accordance with the procedure stipulated in this Article.

According to the Article 160[1] of the Criminal Procedure Code in urgent cases, order could be issued by prosecutor. In this case, an order of a pre-trial investigation judge approving the legitimacy of the order must be obtained within three days from the taking of the decision.

According to General Prosecutor order No. I-383 of December 31, 2012[3], the prosecutor's decision and the investigation judge consent shall not be required to obtain information directly related to telephone numbers or electronic communications terminal equipment, telephone number, email address or network terminal equipment dependency, or to natural or legal person account numbers or bank accounts or dependence of financial and / or payment instruments and persons entitled to dispose of it.

According to the Article 10 of Law on Cyber Security the Police has the right to issue an order to the provider of public communications networks and or public digital communications service provider, digital information hosting service provider and digital service provider to preserve and get information related to the services provided by them which might help detect the type of communications service used, technical measures which were applied and the times of usage, identify the recipient of services, mail address, geographical location address, phone or any other access number, information about accounts and payments made on the basis of service agreement and other information which is available in the location where communications equipment is installed, on the basis of the existing service contract or agreement, and with the court ruling substantiated available, to receive the data of service recipients' flow.

Also please see the information provided for the question 3.

Requests for data production are carried out without undue delay.

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. National competent authority to receive and execute request depends on the applicable procedures and the legal instrument on which the request is based.

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

---

3 https://www.e-tar.lt/portal/lt/legalAct/TAR.FB0E47A36ED6

Acceptable languages: Lithuanian (for EIO: Lithuanian and English); for data preservation in the framework of Budapest Convention: English.