Fiches Belges on electronic evidence – SLOVAK REPUBLIC

1. Definition of electronic evidence

There is no specific legal definition of electronic evidence in the Slovak legislation. The electronic evidence is covered by a general provision on evidence in the Code of Criminal Procedure. Pursuant to Section 119 par. 2 of the Code of Criminal Procedure: „(2) Anything that may contribute to properly clarifying the case and that has been obtained in a lawful manner in compliance with this Act or with the other acts can be used as evidence. The means of evidence are especially hearings of the accused, witnesses, experts witnesses, forensic expert opinions and specialist knowledge statements, verifying testimony on the scene, test identification parade, crime scene reconstruction, investigation experiment, site inspection, objects and documents relevant for criminal proceedings, criminal complaint, information collected using technical means or criminal intelligence checks.“

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

The Slovak Republic is a Party to the Convention on Cybercrime (CETS 185) as well as other major multilateral conventions on mutual legal assistance. Moreover, the Slovak Republic applies the EU mutual recognition instruments including the EIO. As regards electronic evidence, it is possible to apply preservation of such data (Article 29 of the Convention on Cybercrime – Section 90 of the CCP). The data may be provided/disclosed through the EIO, Convention on Cybercrime, any other applicable international instrument or reciprocity. It is also possible to provide spontaneous information within the circumstances of Article 7 of the MLA 2000 Convention or Article 26 of the Convention on Cybercrime.

3. Procedure for obtaining electronic evidence

a. National procedures

Procedure for obtaining electronic evidence is regulated by the Code of Criminal Procedure (Act No. 301/2005 Coll. as amended). Specific regulations on providers are contained in the Act No. 351/2011 as amended on electronic communications. Both acts were affected by the decision of the Constitutional Court PL ÚS 10/2014.

Code of Criminal Procedure:

Section 90 - Storage and Disclosure of Computer Data

(1) If the storage of the stored computer data is necessary for the clarification of the facts necessary for the criminal proceedings, including operating data that is stored through a computer system, the presiding judge and, before the onset of the criminal prosecution or in the preliminary hearing, the public prosecutor, may issue an order that must be justified even by the merits, to the person who possesses or controls such data, or the provider of such services to
a) store such data and maintain the integrity thereof,
b) allow the production or retention of a copy of such data,

c) render access to such data impossible,
d) remove such data from the computer system,
e) release such data for the purposes of the criminal proceedings.

(2) In the order under Subsection 1 Paragraphs a) or c), a period during which the data storage shall be performed must be determined. This period may be up to 90 days, and if its re-storage is necessary, a new order must be issued.

(3) If the storage of the computer data, including the operating data for the purpose of the criminal proceedings, is no longer necessary, the presiding judge and, before the onset of the criminal prosecution or in the preliminary hearing, the public prosecutor, shall issue an order for the revocation of the storage of such data without undue delay.

(4) The order under Subsection 1 through 3 shall be served to the person who possesses or controls such data, or to the provider of such services, and they may be imposed an obligation to maintain the confidentiality of the measures specified in the order.

(5) The person who possesses or controls the computer data shall release such data or the provider of services shall issue the information regarding the services that are in their possession or under their control to those who issued the order under Subsection 1 or to the person referred to in the order under Subsection 1.

Section 115 - Interception and Recording of Telecommunication Operations

(1) In criminal proceedings on a crime, corruption, criminal offences of extremism, a criminal offence of abuse of authority of a public official, a criminal offence of money laundering or another intentional criminal offence, the performance of which is bound by an international treaty, a warrant for the interception and recording of telecommunication operations may be issued if it may be reasonably assumed that it will aid in obtaining all the facts relevant to the criminal proceedings. The warrant may be issued if the purpose pursued may not be attained otherwise or if its attainment in another manner would be considerably hindered. If it is found during the interception and recording of telecommunication operations that the accused has communicated with their defence counsel, such obtained information may not be used for the purpose of the criminal proceedings and must be destroyed in a prescribed manner without undue delay; this shall not apply if it is about information which relates to the matter in which the attorney does not represent the accused as their defence counsel.

(2) The warrant for the interception and recording of telecommunication operations shall be issued by the presiding judge, before the onset of the criminal prosecution, or in the preliminary hearing upon the petition of the public prosecutor, by the judge for the preliminary hearing. If it is a matter that cannot be deferred and the interception and recording of telecommunication operations is not associated with entry into a dwelling and a written warrant from the judge for the preliminary hearing cannot be obtained in advance, the warrant may be issued before the commencement of the criminal prosecution or in the preliminary hearing by the public prosecutor; the warrant must be confirmed by the judge for the preliminary hearing no later than 24 hours from its issue, otherwise it shall expire and the information thus obtained cannot be used for the purposes of the criminal proceedings and must be destroyed in a prescribed

manner without undue delay.

(3) The warrant for the interception and recording of telecommunication operations must be issued in writing and must be justified by its merits, specifically for each user address or device. The warrant must include the determination of the user address or device and the person, if their identity is known, that the interception and recording of telecommunication operations concerns, and the period during which the interception and recording of telecommunication operations will be performed. The interception and recording period may last up to six months. In the preliminary hearing upon the petition of the public prosecutor, this period may be extended by the judge for the preliminary hearing, but always by only two months although it can be done so repeatedly. The interception and recording of telecommunication operations shall be performed by the competent department of the Police Force.

(4) A police officer or the competent department of the Police Force is obligated to systematically examine whether the reasons that led to the issue of the interception and recording of telecommunication operations warrant are still valid. If the reasons have expired, the interception and recording of telecommunication operations must be terminated, even before the lapse of the period referred to in Subsection 3. The person who issued the warrant for the interception and recording of telecommunication operations and, in the preliminary hearing also the public prosecutor, shall be notified.

(5) In criminal proceedings for an intentional criminal offence other than the one referred to in Subsection 1, the presiding judge, before the commencement of the criminal prosecution or in the preliminary hearing, the judge for the preliminary hearing upon the petition of the public prosecutor, may issue a warrant for the interception and recording of telecommunication operations, but only with the consent of the user of the intercepted or recorded telecommunications device.

(6) If the recording of telecommunication operations is to be used as evidence, the literal transcript of the recording shall be enclosed with it, if the prepared recording allows it, which shall be prepared by a member of the Police Force performing the interception, in the extent of the findings crucial for the criminal proceedings, with information on the time, place, authority that prepared such recording, and legality of the interception. The recording of telecommunication operations shall be stored as a whole on file using the appropriate electronic media, copies of which may be requested by the public prosecutor and the accused or their defence counsel. After the completion of the interception and the recording of telecommunication operations, the accused or their defence counsel may receive a transcript of the recording of the telecommunication operations to the extent to which they deem it necessary, at their own expense. The obligations referred to in the first sentence shall apply to them accordingly. The credibility of the transcript shall be assessed by the court. If the transcript of the recording was prepared in the preliminary hearing, the presiding judge may order its completion, which shall be performed by a member of the Police Force referred to in the first sentence. The transcript of the recording of the telecommunication operations is entered into a file that is not classified, signed by the member of the Police Force who prepared it; if the literal transcript of the recording contains classified information, it shall be classified under the regulations on the protection of classified information. The recording of the telecommunication operations may not be used as evidence until after the completion of the interception and

recording of telecommunication operations. In the preliminary hearing, if the circumstances of the case justify it, the recording of the telecommunication operations may be submitted to the court even without the transcript of this recording, provided that the enclosed report details information on the location, time, the authority that prepared such recording and the legality of the interception, as well as on persons that the recording of the telecommunication operations concerns and that the recording of the telecommunication operations is clear.

(7) In a criminal matter other than one in which the interception and recording of telecommunication operations was performed, the recording may be used as evidence only if there is a criminal proceeding for a criminal offence referred to in Subsection 1 in such matter at the same time.

(8) If the interception and recording of telecommunication operations did not find any facts relevant to the criminal proceedings, the law enforcement authority or the competent department of the Police Force must destroy such recordings in the prescribed manner without undue delay. A transcript on the destruction of the recordings shall be entered into the file.

(9) The police officer or public prosecutor by whose decision the matter was finally concluded and, in the proceedings before the court, the presiding judge of the court of first instance shall inform the person stated in Subsection 3, if known, on the destruction of the recordings after the final conclusion of the matter. The information shall contain identification of the court that issued or confirmed the warrant for the interception and recording of telecommunication operations, duration of the interception, and the date of its termination. The information shall also include instruction on the right to file a petition for reviewing the legitimacy of the warrant for the interception and recording of telecommunication operations with the Supreme Court within two months from the delivery of the information. The information shall be provided by the authority by whose decision the matter was finally concluded and, in proceedings before the court, by the presiding judge of the court of first instance within three years from the final conclusion of the criminal prosecution in the given matter.

(10) The information under Subsection 9 shall not be provided by the presiding judge, police officer or public prosecutor to a person who has the possibility of inspecting the file under this Act or in proceedings on a particularly serious crime or crime committed by an organised group, criminal group or terrorist group, or where several persons participated in the commission of the criminal offence and, in relation to at least one of them, the criminal prosecution was not finally concluded, or if the provision of such information could obstruct the purpose of the criminal proceedings.

(11) The provisions of Subsection 1 through 10 shall equally apply to the data that is transmitted through a computer system in real time.

Section 116 - Notification of Data on Telecommunication Operations

(1) In criminal proceedings for an intentional criminal offence for which this Act sets out a prison sentence with an upper penalty limit of at least three years, for a criminal offence of the protection of privacy in the dwelling under Section 194a, fraud under Section 221, dangerous threats under Section 360, stalking under Section 360a,

spread of alarming news under Section 361, incitement under Section 337, endorsement of a criminal offence under Section 338, for a criminal offence by which grievous bodily harm or death was caused or for another intentional criminal offence, the conduct of which is bound by an international treaty, a warrant for the determination and notification of data on telecommunication operations, which is subject to telecommunications privacy, or subject to personal data protection, which is necessary to clarify the facts relevant to the criminal proceedings, may be issued. The warrant may be issued if the purpose pursued may not be attained otherwise or if its attainment in another manner would be considerably hindered.

(2) A warrant for the determination and notification of data on telecommunication operations shall be issued by the presiding judge and, before the commencement of the criminal prosecution or in the preliminary hearing, by the judge for the preliminary hearing upon the petition of the public prosecutor, which must be written and also justified by its merits. The warrant for the determination and notification of data on telecommunication operations must be issued in writing and justified; the warrant shall also include the manner, extent and period for the notification of the data. If the warrant relates to a specific user, it must indicate their identity, if known. Where determination and notification of data on the performed telecommunication operations is not concerned, determination and notification of such data may last no more than six months; this period may be extended by the judge for the preliminary hearing upon a written and justified petition of the public prosecutor in the preliminary hearing, always by two months, and this may be done repeatedly. The warrant for the determination and notification of data on telecommunication operations shall be delivered to the enterprise providing public networks or services.

(3) If the data obtained in the procedure under Subsection 1 and 2 did not ascertain facts relevant to the criminal proceedings, the authority by whose decision the matter was finally concluded shall destroy the data without undue delay; a police officer shall destroy the data after obtaining prior written consent of the public prosecutor. A transcript on the destruction of the data shall be entered into the file.

(4) The police officer or public prosecutor by whose decision the matter was finally concluded and, in proceedings before the court, the presiding judge of the court of first instance, shall inform the person stated in Subsection 2, if known, in writing on the destruction of the data on telecommunication operations after the final conclusion of the matter. The information shall contain identification of the court that issued the warrant for the determination and notification of data on telecommunication operations, and data about the period for which the warrant was executed. The information shall also include instruction on the right to file a petition for reviewing the legitimacy of the warrant for the determination and notification of data on telecommunication operations with the Supreme Court within two months from the delivery of the information. The information shall be provided by the authority by whose decision the matter was finally concluded and, in proceedings before the court, by the presiding judge of the court of first instance, within three years from the final conclusion of the criminal prosecution in the given matter.

(5) The information under Subsection 4 shall not be provided by a presiding judge, police officer or public prosecutor to a person who has the possibility to inspect the file under this Act or in proceedings on a particularly serious crime or crime committed by

an organised group, criminal group or terrorist group, or where several persons participated in the commission of the criminal offence and, in relation to at least one of them, criminal prosecution has not been finally concluded, or if the provision of such information could obstruct the purpose of the criminal proceedings.

(6) The provisions of Subsection 1 through 5 shall equally apply to data transmitted through a computer system.

Act No. 351/2011 Coll. on Electronic communications:

Section 63 paragraphs 6 - 13

(6) Undertaking shall provide prosecuting authorities for purposes of criminal proceedings and other state administration authorities pursuant to § 55 paragraph. 6 for purposes of fulfillment of their tasks under special legislation with data that are subject to telecommunications secrecy pursuant to paragraph 1. letter b) to d).

(7) The data referred to in paragraph 6 shall be provided only upon written request and with the written consent of the lawful judge ("the consent"). Consent may be granted only if the intended purpose cannot be achieved by other means or if its achievement would be considerably more difficult.

(8) Request for consent contains
a) identification of the body of state administration by which the consent is requested,
b) identification data of person concerned if they are known,
c) nature, scope and the time limit for the submission of data according to paragraph 6,
d) the justification of the purpose of providing information according to paragraph 6,
e) information on the previous ineffective or substantially more difficult detection and documentation of activities for which the application is made.

(9) If the request for consent does not contain all items referred to in paragraph 8, the court will not deliver and will return the application to the body of state administration.

(10) The consent shall include a justification and a period no longer than six months, in which the information according to paragraph 6 shall be retained and provided; this period may be prolonged based on the new consent of the court, but each time for not more than six months. Request under the preceding sentence shall include all items referred to in paragraph 8. The decision on consent cannot be appealed against.

(11) The rules of special regulation applies as to which court is competent to give consent under this Article.

(12) If the data referred to in paragraph 6 were not useful in finding facts relevant for the fulfillment of the tasks of the body of state administration, that body of state administration shall immediately destroy them; minutes shall be made in writing on destruction of the data.

(13) Supervision over collection of data by a body of state administration pursuant to paragraph 6 is effectuated by the National Council of the Slovak Republic; the supervision is regulated by a special regulation.

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)

Obtaining the evidence for criminal proceedings is only possible through the mutual legal assistance or based on the EU instruments on mutual recognition.

Preservation requests under Article 29 should be sent through the national 24/7 contact point. Preservation requests must contain the formalities described in Article 29 of the Convention on Cybercrime and must be issued or at least validated by a judicial authority (it may be a prosecutor, a judge or any other competent authority performing judicial functions under the national law of the requesting state).

An assistance may be provided by Eurojust, EJN or EJCN within their mandates.

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

- Convention on Cybercrime, Budapest 23. XI 2001 (CETS 185)
- European Convention on Mutual Assistance in Criminal Matters, Strasbourg 20. IV 1959 (CETS 030) and its two additional protocols
- UN Convention against Transnational Organised Crime (UNTOC), Palermo 2000
- Convention of 29 May 2000 on Mutual Assistance in Criminal Matters between the Member States of the European Union and its Protocol
- Directive 2014/41/EU regarding the European Investigation Order in criminal matters (and the transposing legislation) – only applicable to relevant EU Member States
- other bilateral and multilateral treaties and EU legislation
- reciprocity

5. **competent authority to receive and execute your request**

The competent authorities to receive requests **depend on the applicable instruments.** Requests are sent either directly to the competent authorities (prosecution offices or courts) or to the central authorities (pre-trial stage – General Prosecutor´s Office, trial stage or reciprocity – Ministry of Justice).

The competent prosecutor´s offices to execute the preservation requests and requests for mutual legal assistance are district prosecutor´s offices, where the action should take place.

To ensure the processing of a letter rogatory from a foreign authority for legal assistance, the district prosecutor´s office, under which jurisdiction the requested act

of legal assistance is to be performed, is competent. If the local jurisdiction is given to several public prosecutions, the Ministry of Justice shall send the letters rogatory to the General Prosecutor´s Office for a decision as to which of the public prosecutions shall provide its processing.

Procedure according the EIO is governed by the Act. No. 256/2017 Coll.

Competent prosecutor´s offices for the execution of EIOs are regional prosecutors´ offices. In case of concurrent territorial competences of more regional prosecutor´s offices, the competent is the regional prosecutor´s office which acted as first. In case of doubts the GPO is competent to decide about the territorially competent prosecutor´s office.

If the issuing authority requests the execution of the EIO by the court for the reason of admissibility of evidence in the issuing state a prosecutor submits the EIO for execution in this part to the competent district court. If the EIO only contains investigative measure to be executed by the court due to admissibility of evidence in the issuing state, the EIO should be sent directly to the district court where the action should take place.

6. accepted languages

In principle, requests are accepted in Slovak. Acceptance of requests in foreign languages depends on the applicable treaties or instruments.

For preservation requests a language regime of applicable (comprehensive) MLA treaties is accepted (of those English is the most preferable) as these are considered as a part of MLA system.

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

Although the Slovak legislation (Act No. 351/2011 Coll. on electronic communications contains definitions, we do not see any relevance to provide it here, since disclosure of data require the same conditions.

Obtaining of e-evidence

Obtaining of e-evidence is possible only on the basis of the court order for any type of computer data. This apply to subscriber, traffic/transaction and content data. Conditions for the court order (warrant) are set out **in the Section 116 para 1 of the CCP** (notification of Data on Telecommunication Operations):
In criminal proceedings for an intentional criminal offence for which this Act sets out a prison sentence with an upper penalty limit of at least three years, for a criminal offence of the protection of privacy in the dwelling under Section 194a, fraud under Section 221, dangerous threats under Section 360, stalking under Section 360a, spread of alarming news under Section 361, incitement under Section 337, endorsement of a

criminal offence under Section 338, for a criminal offence by which grievous bodily harm or death was caused or for another intentional criminal offence, the conduct of which is bound by an international treaty, a warrant for the determination and notification of data on telecommunication operations, which is subject to telecommunications privacy, or subject to personal data protection, which is necessary to clarify the facts relevant to the criminal proceedings, may be issued. The warrant may be issued if the purpose pursued may not be attained otherwise or if its attainment in another manner would be considerably hindered.

Conditions for providers are contained in Act No. 351/2011 Coll..

Conditions for obtaining e-evidence **through EIO** are set up in the EIO Directive and in the national transposing legislation - **Act No. 236/2017 Coll. on European investigative order in criminal matters.**

EIO could be issued/executed only for the criminal proceedings for the purpose of gathering or to obtain the evidence and in accordance with the legal order of the Slovak Republic. There are any additional requirements in comparison to the EIO Directive. The Act No. 236/2017 Coll. is *lex specialis* to the Code of Criminal Procedure (as *lex generalis*).

The seizure of a thing/an item is regulated in the Section 38 of the Act. No. 236/2017 Coll. The competent judicial authority usually in 24 hours decides if the EIO could be executed and inform about it the issuing State.

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

The evidence may only be obtained from abroad through MLA or EU mutual recognition instruments.

   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**

Due to data protection regime as well as the fact that only procedural ways to obtain the evidence in criminal proceedings are MLA procedures and procedures based on the mutual recognition instruments, voluntary disclosure is not regulated.

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

There is no mandatory data retention system. The Act No. 351/2011 Coll. as amended on electronic communication does not prescribe any period. Providers retain the data only for the period necessary for their legitimate (business purposes). Some data is not retained at all. Some is retained within a few day or weeks. The period depends on the providers policies.

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

The data is preserved for 90 days. If necessary a new order for extra 90 days may be issued once. A request under Article 29 should be sent via 24/7 contact point. For more information see also 3b and 6. If all formalities are met a request is executed within days (or even hours in urgent cases). However, there is no obligation of providers to have 24/7 services for cooperation with LEA/judicial authorities.

11. **Procedure for data production/ execution deadline**

MLA request or EIO are key basis for data production in the field of international cooperation. For disclosure from providers Section 116 of the CCP is mostly applicable. In other cases, Section 90 of the CCP may apply for disclosure as well. Provisions on international cooperation (Chapter V) of the Code of Criminal Procedure also apply accordingly (for MLA).

The EIO or MLA request in a prescribed language is a precondition for data disclosure.

12. **Concise legal practical information**

E-evidence contains both legal and technical issues. Make sure the request is clear enough in terms of provider concerned and data requested (in terms of data from servers, location of such servers etc.). In more complicated cases it is advisable to contact the EJN/EJCN contact points in order to facilitate the execution.

Please make sure that preservation requests contain the information in accordance with Article 29 of the Convention on Cybercrime and are issued or validated by judicial authority.