EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

HUNGARY

Completed with the support of the EJCN Contact Point

1. Definition of electronic evidence

According to Section 205 (1) of the Hungarian Code on Criminal Procedure (hereinafter HU CCP), 'electronic data' means any representations of facts, information or concepts in a form suitable for processing in a computer system, including programs suitable to cause a computer system to perform a function.
This definition meets the concept of 'computer data' defined in point b) of Article 1 of the Convention on Cybercrime.

Hungarian criminal procedural law draws a distinction between concepts of data and evidence; evidence is the information itself that, as a result of an evaluation process, can be concluded from the data. In other words, data is an evidentiary instrument that carries the information considered evidence.

In essence, electronic evidence originates from electronic data automatically stored, processed or transferred in an information system.

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

Hungarian authorities are able to perform all measures legislated in domestic procedural law (see at point 3.a.). As Hungary is a party to the Convention on Cybercrime (CoC) and has complied with the obligations to ensure a legislation by which measures listed in the procedural law section of CoC are available, all the following measures are possible to perform:
- expedited preservation of stored computer data (due to Article 29, it works without judicial cooperation, through the 24/7 Network)
- expedited preservation and partial disclosure of traffic data
- production order
- search and seizure of stored computer data
- real-time collection of computer data
- interception of content data.

3. Procedure for obtaining electronic evidence
a. National procedures
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)

a.
According to the HU CCP, obtaining electronic evidence in a criminal proceedings is possible

- by collecting data through Open Source Intelligence methods (Section 215 (2) and Section 215 (3) b))
- by requesting data from any legal entities or from entities without legal personality registered under Hungarian law (Section 261)
- by performing a search and seizure (Sections 302, 308 and 315)
- by ordering an ISP or other data holder or controller to preserve the data (Section 316)
- by pursuing wiretapping (both traffic and content data, Section 231 (e))
- by performing real-time collection of computer data (both traffic and content data, Section 231 a))
- by carrying out a secret observation through cameras (Section 231 c)).

b.
Hungarian judicial authorities, by MLA requests based on bilateral or multilateral agreements as well as by EIOs, guarantee the availability of measures listed above. There are also operational contact points to the CoC's 24/7 Network (the National Bureau of Investigation and the Centre for International Cooperation in Criminal Matters) to carry out expedited data preservation and provide assistance.

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

As for expedited data preservation, it is based on Article 29 and 35 of the Convention on Cybercrime, any other measures listed above are available under provisions on mutual legal assistance in criminal matters of bilateral and multilateral agreements and the 2014/14/EU Directive on EIO.

5. competent authority to receive and execute your request

According to the list published by the European Council (participants to the CoC, 24/7 contact point authorities) both the National Bureau of Investigation and the Centre for International Cooperation in Criminal Matters are competent to perform expedited data preservation.
Regarding other measures, there is not a single specialized authority to receive or execute the requests.

6. accepted languages

Hungarian and English, in regards of EIOs: Hungarian, English, French, German

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

In domestic criminal proceedings, there is not any difference between the various categories of electronic data in terms of whether they can be obtained by taking coercive measures or by submitting a request, nor are there requirements and thresholds for access. Classification of data has significance only when picking the proper technical method for performing an investigative measure.

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

Computer data obtained by voluntary dislosure from foreign ISPs are considered as intelligence. In order to turn them into evidence, an MLA request is necessary.

   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

Providing data directly by Hungarian OSPs to foreign authorities are voluntary and there is not any legislation or procedure to follow in this regard.

9. Data retention periods (including procedures for extensions)

According to Section 159/A of Act C of 2003 on electronic communications
(1) Electronic communications network operators and providers of electronic communications service shall be required - for the purpose of compliance with any request made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorization conferred in specific other legislation, with a view to discharge their respective duties - to retain the data generated or processed by the service provider in connection with the provision of electronic communications services relating to the subscribers or users of such electronic communications services:
a) the subscriber's personal data contained in the individual subscriber contract related to fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these;
b) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, the telephone number allocated to the terminal equipment of the user or subscriber or to the subscriber access point, or the user ID or any technical identifier fixed in the subscriber contract or otherwise assigned to the subscriber or user by the provider of electronic communications services;
c) in connection with fixed network telephony services, fixed internet access services, or the combination of these, the address where the terminal equipment of the user or subscriber or the subscriber access point is installed, and the type of equipment;
d) in connection with fixed network telephony and mobile telephony services, internet access, internet telephony, internet mail services, or the combination of these, the telephone numbers of the users and subscribers participating in the communication, their technical means of identification, user IDs, type of electronic communication services involved, and the data necessary to identify the date, time and duration of a communication;
e) in connection with fixed network telephony and mobile telephony services, or the combination of these, in cases involving call forwarding or call transfer, the subscriber or user number or numbers to which the call is routed;
f) in connection with mobile telephony services, concerning the equipment used at the time of communication, the International Mobile Equipment Identity (IMEI) of the calling and the called party, and the International Mobile Subscriber Identity (IMSI) of the calling and the called party;
g) in connection with mobile telephony services, the location label (cell ID) and network identifier at the start of the communication, and the data identifying the geographic location of cells by reference to their location labels (cell ID) during the period when the service was provided;
h) in connection with internet mail services and internet telephony services, or the combination of these, the data referred to in Paragraph d) of the intended recipient(s) of the communication;
i) in connection with internet access, internet mail services, internet telephony services, or the combination of these, type of the electronic communication service, the date and time of the log-in and log-off by the subscriber or, together with the IP address allocated to the communication, and the user ID of the subscriber or registered user, including the calling number;
j) in connection with internet access, internet mail services and internet telephony services, or the combination of these, the data necessary to trace any changes made in the unique identifiers of subscribers and users by the provider of electronic communications services (IP address, port number);
k) in the case of pre-paid anonymous mobile telephony services, the date and time of the initial activation of the service and the location label (cell ID) from which the service was activated.
(2) The obligation to retain data provided for in Subsection (1) shall include the retention of the data specified in Subsection (1) relating to unsuccessful call attempts.

(3) Providers of electronic communications services, for the purposes of compliance with the obligation of disclosure referred to in Subsection (1), shall retain the data specified in Paragraphs a)-c) of Subsection (1) for a period of one year following termination of the subscriber contract, the data specified in Paragraphs d)-k) of Subsection (1) for a period of one year following the time they were generated, and the data specified in Subsection (2) for a period of six months following the time they were generated.

Section 157
(1) With the exceptions set out in Subsection (2) of this Section and in Subsection (1) of Section 159/A, traffic data relating to subscribers and users processed and stored by the provider of electronic communications services while providing such services must be erased or made anonymous when it is no longer needed.
(2) Electronic communications service providers shall be authorized to process the following data for subscribers and users for the purposes of billing for calls, collecting the related charges and for keeping the subscriber contracts up to date:
a) the data referred to in Paragraph a) of Subsection (5) of Section 129;
b) the telephone number or other identifier of the subscriber terminal;
c) the address of the subscriber and the type of terminal equipment;
d) total units chargeable for the billing period;
e) calling and called subscriber numbers;
f) the type of calls or other services, their direction, start time, the duration of conversations or the size of data transmitted, the International Mobile Equipment Identity (IMEI) of the network and cell providing the service and of the telephone set used for making use of the service provided in the case of mobile radio telephone networks, and for IP networks the identifiers used;
g) the date of call or other services provided;
h) data connected with the payment of charges or charges in arrears;
i) events of the termination of a subscriber contract if terminated with debts outstanding;
j) data relating to other, non-electronic communications services, in particular to the billing of charges therefor, that may be used by subscribers and users in the case of telephone services;
k) data the service provider has obtained in connection with the unlawful use of subscriber terminal equipment, or any attempt to do so, for accessing subscriber services in the electronic communications network, in particular when such equipment has been barred by its rightful owner.
(3) The data referred to in Subsection (2) may be processed for the purposes mentioned in Subsection (2) until the term of limitation established by Subsection (2) of Section 143 for claims arising from subscriber contracts
(10) **Providers of electronic communications services shall be required to disclose or make available the data in their possession according to Subsection (2) upon request made by the investigating authority, the public prosecutor, the court or the national security service pursuant to the authorization conferred in specific other legislation, to the extent required to discharge their respective duties.**

10. Procedure for data preservation/execution deadline

In case of an incoming request sent via 24/7 Network under Articles 29 and 35 of CoC, the National Bureau of Investigation prepares a decision on data preservation and presents it to the prosecutor for countersigning. Execution of the decision follows at the respective ISP. It only takes a couples of hours or a few days at maximum, depending on the need for clarification.

In case of other requests based on mutual legal assistance treaties and in domestic proceedings, under Section 316 of the HU CCP, the investigative authority, the prosecutor or the judge may order the ISP to preserve data for a maximum period of three months.

EUROPEAN JUDICIAL NETWORK

11. Procedure for data production/ execution deadline

Under section 261 of the HU CCP, data sought in a criminal proceedings must be provided by ISPs or other data holders and data controllers by a written request of the investigative authority, the prosecutor or the judge within 1 to 30 days when the request is fulfilled in electronic ways and 8 to 30 days when the answer is provided in other forms (e.g. printed).

This procedure is also to be followed in international judicial cooperation.

12. Concise legal practical information