EUROPEAN JUDICIAL NETWORK

Fiches Belges on electronic evidence

Bulgaria

1. Definition of electronic evidence

The BG Criminal Procedure Code does not define legally "electronic evidence". However, Bulgaria signed and ratified the Council of Europe Convention on Cybercrime (entry into force: 01/08/2005), also called 'Budapest Convention on Cybercrime' (or simply 'Budapest Convention') which refers to electronic evidence as evidence that can be collected in electronic form of a criminal offence. There is case-law defining "electronic evidence" as any type of digital data that can be used to help establish (or refute) whether a crime has been committed.

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

a. Expedited preservation (Art. 29 Budapest Convention)
b. Expedited disclosure of traffic data (Art. 30 Budapest Convention)
c. Production orders/access to data (Art. 31 Budapest Convention)
d. General MLA or EIO

In case of absence of bilateral/multilateral agreements on mutual legal assistance, could be the options for sending or receiving request for retained data:

e. Reciprocity
f. Spontaneous information (Art. 26 Budapest Convention)
g. Trans-border access (Art. 32 Budapest Convention)
h. Spontaneous information (Art. 7 EU Convention)

3. Procedure for obtaining electronic evidence

a. National procedures – described in Criminal Procedure Code.

- *General rule (Article 159):*

Upon request of the court or the pre-trial authorities, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data and other data, that may be of significance to the case.

- *Gathering of the electronic communication (Article 159a):*

Upon request by a court as part of court proceedings or based on motivated order by a judge of the respective court of first instance, issued by request of the supervising prosecutor of pre-trial proceedings the enterprises, providing public electronic communication networks and/or services shall make available the data, generated in the course of performance of their activities, which may be required for:

- tracing and identification of the source of the communication link;
- identification of the direction of the communication link;
- identification of the date, hour and duration of the communication link;
- identification of the type of the communication link;
- identification of the terminal electronic communication device of the user of that presenting itself as its terminal device;
- establishment of an identification code of the cells used.

The above-mentioned data shall be collected where required for investigation of serious premeditated crimes.

The request of the supervising prosecutor shall be substantiated and must certainly contain:

- information concerning the crime, for the investigation of which data concerning the traffic is required;
- description of the circumstances, on which the request is based;
- data regarding the individuals, for whom data concerning the traffic is required;
- the time period, which the information summary must cover;
- the investigating authority, to which the data must be provided.

The court shall indicate in its order:

- data, which must be reflected in the information summary;
- the time period, which the information summary must cover;
- the investigating authority, to which the data must be provided.

The time period, for which provision of the above-mentioned data may be requested and authorised, shall not exceed 6 months.

If the information summary contains data, which is not related to the circumstances under the case and does not contribute to their clarification, upon motivated written request of the supervising prosecutor the judge, who issued the authorisation, shall order the destruction of that material. The destruction shall be performed under procedure, approved by the Chief Prosecutor. Within 7 days of receipt of such order the enterprises and the supervising prosecutor shall submit to the judge who issued it the protocols of destruction of the data.

- *Search and seizure (Articles 160-163):*

In pre-trial proceedings search and seizure shall be performed with an authorisation by a judge from the respective first instance court or a judge from the first-instance court in the area of which the action is taken, upon request of the prosecutor. In cases of urgency, where this is the only possible way to collect and keep evidence, the pre-trial authorities may perform physical examination without authorisation , the record of the investigative action being submitted for approval by the supervising prosecutor to the judge forthwith, but not later than 24 hours thereafter.

The computerized information systems containing computerized data seized shall be shown to the certifying witnesses and the other attending persons. Where necessary, these shall be wrapped and sealed at the location where they had been seized.

Seizure of computerized data shall be operated through record on paper or another carrier. In case of a paper carrier, each page shall be signed by. In other cases the carrier shall be sealed with a note stating: the case, the body performing the seizure, the location, date, and names of all individuals present who shall sign it. Carriers will only be unsealed with the authorisation of the prosecutor for the needs of the investigation, which shall be carried out in presence of certifying witnesses and an expert- technical assistant. In court proceedings carriers shall be unsealed upon decision of the court by an expert technical assistant.

- *Interception and seizure of correspondence (Article 165):*

Interception and seizure of correspondence (including electronic correspondence) shall be allowed only where this is necessary for disclosure or prevention of serious crime.

Interception and seizure of correspondence in pre-trial proceedings shall be performed upon request of the prosecutor with the authorisation of a judge from the respective first instance court or a judge from the court in the area of which the action is taken.

In urgent cases, when this is the only option to collect and preserve evidence in investigating crimes under Article 108a and Article 354a of the Criminal Code, the pre-trial authorities may intercept undelivered correspondence without the authorisation. The supervising prosecutor shall - promptly, but no later than 24 hours - submit the records of the executed action to a judge of the responsible court, together with a reasoned written request for seizure of the intercepted correspondence. The

seizure shall be effected on the basis of a reasoned written authorisation of the judge who shall issue a ruling promptly, but no later than 24 hours. If rejecting the seizure, the judge shall also rule on the intercepted correspondence.
In court proceedings search and seizure of correspondence shall be performed by a decision of the court which is trying the case.
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)

- **Police channels: Europol/Interpol/Sienna/Liaison and foreign liaison officers:** to obtain (basic) subscriber information
- **BG 24/7-channel/network (Budapest Convention):** urgent preservation requests to seize volatile subscriber information/traffic data/content (only with MLAT-guarantee: the available data will be preserved/seized and will only be provided after receiving the MLAT/EIO in 60 days)
- **Article 18 Budapest Convention:** on a voluntary basis (most companies established in Bulgaria supply, however, only on the basis of a request for judicial assistance – to cover themselves against the customer and because of GPDR-issues)
- **General MLAT** (COE and EU treaties; + UN Treaties and bilateral treaties)

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

a. EU Directive 2014/41/EU, with the European Investigation Order (EIO), was implemented in BG law, *effective from 23/02/ 2018*.

b. Budapest Convention

NB. For countries who have not implemented this EU Directive 2014/41/EU:

c. EU Convention on Mutual Assistance in criminal matters between the member states of the European Union (29 May 2000);

d. European Convention on Mutual Assistance in criminal matters (Strasbourg, 1959 and additional protocols);

e. other bilateral and multilateral treaties.

5. Competent authority to receive and execute your request

a. EU Directive 2014/41/EU

The competent authorities to receive an EIO:
• With regard to pre-trial criminal proceedings: a prosecutor of the respective District Prosecutor's Office or Military District Prosecutor's Office within whose judicial area of competence the relevant investigative measure or other procedural measures are requested to be carried out, of evidence which is already in possession is requested to be transferred, or a prosecutor of the Specialized Prosecutor`s Office.
• With regard to a trial itself: a judge of the respective District Court or Military District Court within whose judicial area of competence the relevant investigative measure or other procedural measures are requested to be carried out, of evidence which is already in possession is requested to be transferred, or a judge of the Specialized Criminal Court.
NB. The executing authorities are the same as receiving authorities.
The contact details of all District prosecutors' offices and courts are available on the EJN Website.

b. Budapest Convention

In accordance with Article 35, paragraph 1, of the Convention, BG designates the General Directorate for Combating Organized Crime under the Ministry of Interior to perform the functions of point of contact for the purpose of investigations concerning cybercrime:

Cybercrime Department,
General Directorate Combating Organised Crime - Ministry of Interior.
E-mail address: ncp@cybercrime.bg
Mobile: +359 888 94 18 51.

6. Accepted languages

Bulgarian.
Otherwise: One of the official languages of the Council of Europe, but preferably in English.

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

a. Subscriber data – Basically, personal and some metadata/access data that serve to identify a subscriber or customer, such as the (user)name, date of birth, postal address, gender, type and kind of service (e.g. network provider, VPS- or Dedicated Server, physical location of the server), administrative features (sometimes: bank account), telephone number, email address or IP address at the time of registration, registration date etc.

b. Traffic data – all (transactional) data that relates to the (provision of a) service and its distribution e.g.: the source and destination of the IP address, source and destination port (tcp/udp), timestamp, size IP packet (bytes). (Simply saying: logfiles: date, time, duration, route, date, time of use).
Threshold: because of this intrusive measure (and invasion of privacy), traffic data can only be obtained for serious offences (punishable by more than 5 years imprisonment or life imprisonment), committed intentionally (knowingly), and if proportionate. An explanation from the issuing state with regard to the necessity of content in relation to the investigation is requested.

c. Content data – any stored data in a digital format (text, voice, videos, images, and sound other than subscriber or traffic data).
Threshold: if this data is related to any kind of correspondence, then it can be obtained for serious offences (punishable by more than 5 years imprisonment or life imprisonment), and if proportionate. Basically, it requires a prior court approval. Only in urgent cases, when this is the only option to collect and preserve evidence in investigating crimes under Article 108a and Article 354a of the Criminal Code, the pre-trial authorities may intercept undelivered correspondence without a prior court authorisation. However, prosecutor in charge shall - promptly, but no later than 24 hours - submit the records of the executed action to a judge of the responsible court, together with a reasoned written request for seizure of the intercepted correspondence. An explanation from the issuing state with regard to the necessity of content in relation to the investigation is requested.

8. Voluntary-disclosure:

a. As issuing state: Admissibility of the electronic evidence obtained by voluntary disclosure.
Admissible, if the conditions of subparagraph (b) below are fulfilled (the service provider abroad has access to the subscriber data and provides also services in Bulgaria, and if there is no violation of sovereignty).

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.
Only on a voluntary basis (in the light of Budapest Convention), no enforcement action will be taken. Only in cases where it concerns subscriber information, of a service provider established in the

Bulgaria, requested by a judicial authority of another contracting party, and when the service provider has also access to these data. Without infringing the sovereignty of the other contracting party.

9. Data retention periods (including procedures for extensions)

Execution deadline: the deadlines mentioned in the Budapest Convention (three months which can be prolonged up to six months in total) or the EU Directive 2014/41/EU (EIO).

10. Procedure for data preservation/execution deadline

Execution deadline: the deadlines mentioned in the Budapest Convention (six months) or the EU Directive 2014/41/EU (EIO).

11. Procedure for data production/ execution deadline

Execution deadline: the deadlines mentioned in the Budapest Convention or the EU Directive 2014/41/EU (EIO).

12. Concise legal practical information

a. EIO:

Where an EIO requests the carrying out of an investigative measure or other procedural measures, which extend to multiple judicial districts, the authority competent to recognise any such order shall be the authority within whose judicial district the most urgent measure is to be carried out.

b. Budapest Convention:

In accordance with Article 14, paragraph 3, BG reserves the right to apply the measures referred to in Article 20 only to serious offences, as they are defined by the Bulgarian Criminal Code.

In accordance with Article 24, paragraph 7.a, BG designates the Ministry of Justice as the Central Authority responsible for making or receiving requests for extradition, and the Supreme Cassation Prosecutor's Office as the Central Authority responsible for making and receiving requests for provisional arrest.

In accordance with Article 27, paragraph 2.c, of the Convention, BG designates the following Central Authorities responsible for sending and answering requests for mutual assistance:

– the Supreme Cassation Prosecutor's Office – in respect of requests for mutual assistance at the stage of pre-trial proceeding;

– the Ministry of Justice – in respect of requests for mutual assistance at the stage of the trial. The MLA following up the 24/7-request should include an information which police authority was executed the 24/7-request.