Improving criminal justice in cyberspace

Fields marked with * are mandatory.

QUESTIONNAIRE for EU MEMBER STATES following the 9 June 2016 Conclusions of the JHA Council on improving criminal justice in cyberspace[1]

This questionnaire is designed to provide further information to the European Commission Task Force on Cross-border Access to Electronic-Evidence, in order to facilitate swift progress of our work. We would be grateful for receiving your replies by Friday 16 September 2016.

Whereas some of the questions mainly refer to the legal framework, other questions are more related to current (working) practices in your Member State. The diversity in questions may require you to involve multiple organisations, including e.g. your responsible ministry, prosecutors and / or your national or regional police.

We are aware that you receive many questionnaires, including on these issues. Therefore, where you have provided information already under GENVAL or the Council of Europe, please feel free to simply refer us to answers already provided elsewhere. As the picture is not yet complete across Member States we could not altogether avoid certain questions. If you would like to share existing documents or responses to other questionnaires with us, please feel free to upload them here or to email them to us at **home-cybercrime@ec.europa.eu**.

If you prefer to respond to all or parts of the questionnaire in a separate document, you can download a PDF of this questionnaire by clicking on the link to the right and email your response to **home-cybercrime@ec.europa.eu**. You can also contact us at that email address for a Word version.

We very much appreciate your time and efforts and would like to thank you for your participation. Your contribution is a key element in our effort to address the existing problems.

The E-Evidence Task Force

[1] The electronic version of the questionnaire is available at: https://ec.europa.eu/eusurvey/runner/eevidence

Administrative questions

I. Please indicate on behalf of which EU Member State you are responding to the questionnaire*

☐ Austria
☐ Belgium
+ **Bulgaria**
☐ Croatia
☐ Cyprus
☐ Czech Republic
☐ Denmark
☐ Estonia
☐ Finland
☐ France
☐ Germany
☐ Greece
☐ Hungary
☐ Ireland
☐ Italy
☐ Latvia
☐ Lithuania
☐ Luxembourg
☐ Malta
☐ Netherlands
☐ Poland
☐ Portugal
☐ Romania
☐ Slovak Republic
☐ Slovenia
☐ Spain
☐ Sweden
☐ United Kingdom

II. Please indicate which organisation you are representing *

Supreme Cassation Prosecutor's Office of Republic of Bulgaria

III. Please provide your contact details (name, e-mail address, phone number)*

IV. Did you coordinate your response to the questionnaire amongst different organisations in your Member State? *

+ **Yes**
☐ No

IVa. If yes, could you please indicate amongst which organisations you coordinated your response to the questionnaire?

General Directorate "Combating organized crime"- Ministry of Interior /GDCOC-MoI/

Optional inclusion of files

V. Please provide any details about the file(s) you are including

Va. Please upload your file(s)

[please use the EU Survey website (https://ec.europa.eu/eusurvey/runner/eevidence)]

1. Direct cooperation with service providers for obtaining access to electronic evidence

Part 1 of the questionnaire only concerns direct cooperation between law enforcement authorities and private sector service providers (e.g. providers of telecommunications services or providers of cloud services).

It may concern both mandatory and voluntary cooperation, depending on whether there is (i.e. search warrant) or there is no legal title for compelling the service provider to disclose the electronic evidence.

It does not cover situations where requests are made between authorities from a requesting and a receiving state, e.g. in the framework of a mutual legal assistance or mutual recognition procedure (see Part 2 of the questionnaire).

1.1 Normal practice within your domestic jurisdiction

1. What is the relevant legal framework for direct cooperation requests in your Member State? Could you please copy or include reference to the relevant provision(s) in your legislation?

There is no legal framework for direct cooperation between law enforcement authorities and private sector service providers.

2. For these direct cooperation requests, is there a difference in your legal framework between providers of telecommunications services and providers of information society services (e.g. cloud service providers)?

……

3a. How many domestic requests for direct cooperation are made per year by your authorities? Could you please specify the number of requests per section of the applicable legal framework and type of service provider?

none

3b. Which are the "top" service providers in terms of numbers of domestic requests for direct cooperation? Please include the names of the "top" 5 service providers.

……

1.2. Practice when the service provider is outside your domestic jurisdiction

4. How do you distinguish between domestic and foreign service providers when making a request?

+ **Main seat of the service provider in question**

☐ Place where services are offered

☐ Place where data is stored

☐ Other criteria

4a. If you selected "Other criteria", please specify:

5. Do authorities from your Member State make direct requests to service providers in another EU Member State or in third countries?
+ **Yes, both in EU Member States and third countries**
☐ Yes, but only in other EU Member States
☐ Yes, but only in third countries
☐ No, none of the above

5a. If yes, please indicate which third countries (i.e. outside the EU) are most relevant for you in this context:

USA

6. Does your domestic law address such direct requests from your authorities across borders specifically? Or do you apply the same framework as for domestic requests?
+ **The same legal framework**
☐ Regulated specifically

6a. If regulated specifically, please copy or reference the relevant article(s):

7. Are direct requests sent from your country directly to a service provider in another country considered mandatory or voluntary for the provider to comply with?
☐ Mandatory
+ **Voluntary**

7a. In case they are mandatory, can and do you enforce them, legally and in practice? Could you please explain how?

……

8. Does your domestic law allow service providers established in your Member State to respond to direct requests from law enforcement authorities from another EU Member Sate or third countries?
☐ Yes, both from EU Member States and third countries
☐ Yes, but only from other EU Member States
☐ Yes, but only from third countries
+ **No, this is not allowed**

8a. Please copy or reference the relevant article(s) providing for the legal basis to allow / **prohibit** service providers to do so:

Article 251d **.** Electronic Communications Act

(New, SG No. 24/2015, effective 31.03.2015) (1) The access to the data under Article 251b, Paragraph 1 shall be implemented after permission by the chairperson of the district court or by a judge authorized thereby at the whereabouts of the seat of the body that requested access, for which an order for provision of access to the data shall be issued.
(2) The access to data under Article 251b, Paragraph 1, which pertains to a chairman of a district court, to his/her brother or sister, spouse or a person with whom he/she is in factual cohabitation

of an ascending or descending order, shall be implemented after permission by the chairman of the relevant regional court.

(3) The order under Paragraphs 1 and 2 shall be properly reasoned and shall obligatorily contain:

1. the data that must be reflected in the reply to the information query;

2. the time period covered by the information query;

3. the designated official whom the data is to be provided to;

4. the name, position and signature of the judge.

(4) A special non-public register shall be kept for the reasoned permissions or refusals decreed at the respective district courts.

(5) For the needs of the penal procedure, the data under Article 251b, Paragraph 1 shall be provided to the court and to the bodies of the pre-judicial procedure under the terms and according to the procedure of the Penal Procedures Code.

Penal Procedures Code

Article 159

(1) (Redesignated from Article 159, SG No. 32/2010, effective 28.05.2010, amended, SG No. 24/2015, effective 31.03.2015) 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.
(2) (New, SG No. 32/2010, effective 28.05.2010) The pre-trial authorities or the court may request that the European Anti-fraud Office provide them with the reports and enclosures thereof regarding any investigations conducted by the Office.

Submission of data by enterprises, providing public electronic communication networks and/or services

Article 159a

(New, SG No. 24/2015, effective 31.03.2015)
(1) 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:
1. tracing and identification of the source of the communication link;
2. identification of the direction of the communication link;
3. identification of the date, hour and duration of the communication link;
4. identification of the type of the communication link;
5. identification of the terminal electronic communication device of the user of of that presenting itself as its terminal device;
6. establishment of an identification code of the cells used.
(2) The data under Paragraph 1 shall be collected where required for investigation of serious premeditated crimes.
(3) The request of the supervising prosecutor under Paragraph 1 shall be substantiated and must certainly contain:
1. information concerning the crime, for the investigation of which data concerning the traffic is required;
2. description of the circumstances, on which the request is based;
3. data regarding the individuals, for whom data concerning the traffic is required;
4. the time period, which the information summary must cover;
5. the investigating authority, to which the data must be provided.
(4) The court shall indicate in the order under Paragraph 1:
1. data, which must be reflected in the information summary;

2. the time period, which the information summary must cover;
3. the investigating authority, to which the data must be provided.
(5) The time period, for which provision of the data under Paragraph 1 may be requested and authorized, shall not exceed 6 months.
(6) 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 authorization, 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 under Paragraph 1 and the supervising prosecutor shall submit to the judge who issued it the protocols of destruction of the data.

Grounds for and purpose of the search

Article 160

(1) Should there be sufficient reasons to assume that in certain premises or on certain persons objects, papers or computerized information systems containing computerized data may be found, which may be of significance to the ease, searches shall be conducted for their discovery and seizure.
(2) A search may also be conducted for the purpose of finding a person or a body.

9. Do you have a definition (legal or administrative/practical) of different types of data for law enforcement requests? Does your legal framework distinguish between different types of electronic evidence (e.g. subscriber data, traffic data, content data)?

+Yes

☐ No

9a. If yes, please provide us with the definition(s):

Electronic Communication Act

Traffic Data

Article 248. (1) (Amended and supplemented, SG No. 105/2011, effective 29.12.2011)

The undertakings providing public electronic communications networks and/or services, including networks supporting data collection and identification devices, may process data on users where such data are designated directly for the provision of electronic communications services.
(2) The data on users shall include:
1. **traffic data**: data necessary for the provision of electronic communications services, for billing, for the formation of the subscriber bills, as well as for proving their reliability:
(a) number of the calling end-user and number of the called end-user, card number if electronic pre-payment cards are used;
(b) start and end of the call, specified by date and time, with accuracy up to the second, to the extent technically feasible, and/or, in case of data transfer, volume of the transferred data, for billing purposes;
(c) type of the service provided;
(d) points of interconnection upon establishment of the call, start and end of the use of the said points, specified by date and hour, with accuracy up to the second, to the extent technically feasible;
(e) data on the type of connection or time zones and geographical areas, necessary for billing purposes;
(f) location of a user of a service provided over a mobile network, including where a roaming service is provided;

.....

Article 251b. (New, SG No. 24/2015, effective 31.03.2015) (1) The undertakings providing public electronic communication networks and/or services shall store for a period of 6 months data created or processed in the process of their activity which is necessary for:

1. tracing and identifying the connection source;

2. identifying the direction of the connection;

3. identifying the date, time and duration of the connection;

4. identifying the type of the connection;

5. identifying the terminal electronic communication device of the consumer or of the device which purports to be the terminal device of the consumer;

6. establishing an identifier of the cells used.

(2) The data under Paragraph 1 shall be stored for the needs of national security and for prevention, detection and investigation of serious crimes.

(3) Other data, including the data disclosing the content of the communications cannot be stored according to this procedure.

(4) The data under Paragraph 1 shall be processed and stored in accordance with the requirements of the Personal Data Protection Act.

Article 251i. (New, SG No. 24/2015, effective 31.03.2015) (1) The data under Article 251b, Paragraph 1, Item 1 shall be:
1. in the case of a public telephone service – the caller telephone number and data for identification of the subscriber or user;
2. in the case of internet access, internet electronic mail and internet telephony – an identifier assigned to the user, an identifier of the user and a telephone number determined for each communication entering the public telephone network, data for identification of the subscriber or user, for whom an IP address, an identifier of the user or a telephone number have been determined at the time of the connection.
(2) The data under Article 251b, Paragraph 1, Item 2 shall be:
1. in the case of a public telephone service – dialed number (called telephone number) and in the cases of supplementary services such as re-routing or transfer of the call, a number or numbers to which the call is routed and data for identification of the subscriber or user;
2. in the case of internet electronic mail and internet telephony – an identifier of the user or a telephone number of the recipient(s) of an internet telephony call, data for identification of the subscriber or user and an identifier of the recipient for whom the communication is intended.
(3) The data under Article 251b, Paragraph 1, Item 3 shall be:
1. in the case of public telephone service – the date and time of the start and end of the connection;
2. in the case of internet access, internet electronic mail and internet telephony – the date and time of the log-in and log-off the internet access service, based on a certain time zone, together with the IP address, be it dynamic or static, determined for the connection by the internet access service provider and the identifier of the subscriber or user, the date and time of the log-in and log-off the internet electronic mail service or the internet telephony service, based on a certain time zone.
(4) The data under Article 251b, Paragraph 1, Item 4 shall be:
1. the type of the public telephone service used;
2. the internet service used in the case of internet electronic mail or internet telephony.
(5) The data under Article 251b, Paragraph 1, Item 5 shall be:
1. in the case of fixed-line telephony service – the data about the calling phone number and the called telephone number;
2. in the case of a public telephone service, provided via a mobile terrestrial network – data about the calling and the called telephone number; an International Mobile Subscriber Identity (IMSI) of the calling party; an International Mobile Subscriber Identity (IMSI) of the called party; an International Mobile Equipment Identity (IMEI) of the mobile electronic communications terminal equipment of the calling party; an International Mobile Equipment Identity (IMEI) of the mobile electronic communication terminal equipment of the called party; in the case of prepaid services – the date and time of the initial activation of the service and a location label – an identifier of the cell from which the service is activated and an identifier for identification of the subscriber or user;

3. in the case of internet access, internet electronic mail and internet telephony – the calling telephone number for dial-up access, digital subscriber line (DSL) or other end point of the originator of the connection.
(6) The data under Article 251b, Paragraph 1, Item 6 shall be: administrative addresses of cells of a mobile terrestrial electronic communication network from which a call was generated or in which a call was terminated.

……..

Subscriber data

Article 248. (1) (Amended and supplemented, SG No. 105/2011, effective 29.12.2011)

The undertakings providing public electronic communications networks and/or services, including networks supporting data collection and identification devices, may process data on users where such data are designated directly for the provision of electronic communications services.
(2) The data on users shall include:
……
2. data necessary for the formation of subscriber bills, as well as for proving the reliability of the said bills, including the following data:
(a) **data on the subscriber**: in respect of natural persons: forename, patronymic and surname, Standard Public Registry Personal Number and in respect of non-resident persons, Personal Number, in respect of legal persons and of sole trader natural persons: business name, registered office, address of the place of management and relevant identification code;
(b) type of electronic communications services used;
(c) total number of price units charged for the period of formation of the bill in case of periodic payment;
(d) price of the services used for the relevant period;
(e) information related to the option for payment chosen by the subscriber and the payments made and payments due;
(f) information regarding changes in the use of the service: restriction of use, lapse of a restriction;
3. location data: data processed in electronic communications networks giving the geographic position of the electronic communications terminal equipment of the user.

10. What kind of data can be requested directly from service providers according to your domestic law / the law applicable to the service provider?
☐Subscriber data
☐Traffic data
☐ Content data
☐ Other data

None of the indicated kind of data can be requested directly from service providers according the Bulgarian law.

10a. If you selected "Other data", please explain which type or category of data:

……

11. Do you limit direct requests to cases with specific (e.g. exigent) circumstances or to specific (e.g. serious) crimes?
☐ Yes
+ **No**

11a. If yes, please explain:

12. What is the typical process in your Member State for making a direct request? Which authority typically initiates a request? Which other authorities are involved in processing the request?

LEA – Ministry of Interior

13. Are these requests made in electronic form (e.g. by e-mail or sent through an online portal)? How are these requests tracked? Is there a central repository of requests that is managed by one single authority?

The requests are made in electronic form - by e-mail or sent through an online portal

14. Do any specific agreements on direct requests exist (or are currently being negotiated) between your authorities and foreign service providers?

☐ Yes

+ **No**

14a. If yes, could you disclose which service providers your authorities have such an agreement with? How are these agreements established? What is included in these agreements? Could you please explain?

……

15. For these requests that go beyond your domestic jurisdiction, what is the current practice of your authorities? How many requests are made per year? Which are the "top" service providers in terms of numbers of requests? For these questions, could you please make a distinction between requests within the EU and request outside the EU?

Facebook is in the list of the "top" service providers, which receive direct requests from our LEA

16. What is the average timeframe to obtain data through direct requests to service providers? Are there any fixed deadlines that you include in your request? Do service providers commit to respect certain deadlines?

We don’t include fixed deadlines in our request.
We can’t show average timeframe for obtaining data through direct requests, because it varies.

17. What are the means of transmission of evidence gathered in response to direct request?

☐ Paper (letter)

☐ Disks (optical or magnetic)

☐ Fax

+Normal email

+ Web portal

☐ Secure channel (encrypted email, special ftp, etc.)

☐ Other

17a. If you selected "Other", please specify:

18. Is information gathered through direct requests admissible as evidence in court in your Member State?
☐ Yes
+**No**
☐ It depends on other conditions

18a. If you selected "Yes", could you please provide any article(s) that (either implicitly or explicitly) provide for that? In addition, if addressed by case law, could you please include references to relevant decision(s)?

…….

18b. If you selected "No" or "It depends on other conditions", please explain:

2. Mutual Legal Assistance

Part 2 of the questionnaire concerns requests for electronic evidence between authorities of a requesting and a receiving state (Mutual Legal Assistance or Mutual Recognition procedures).

19. What is the legal framework in your Member State for Mutual Legal Assistance requests for third countries?
+**Budapest Cybercrime Convention**
☐ Other multilateral conventions
☐ Bilateral agreements

19a. If you selected "Other multilateral conventions", please specify:

……..

19b. If you selected "Bilateral agreements", please specify with which countries:

……..

20. How many Mutual Legal Assistance requests for electronic evidence to third countries are made by your authorities per year? Which are the "top" third countries that you send requests to (outside the EU)?

The last 8 years the numbers of the requests for electronic evidence to third countries, made by Bulgarian authorities vary from 1 to 8 per year. Most of them are made to USA.

21. What is the typical process in your Member State for making a Mutual Legal Assistance request to a third country? Which authority initiates such a request? Which other authorities are involved?

Prosecutor's offices initiate Mutual Legal Assistance requests to third countries

22. What kind of electronic evidence do you usually request on the basis of Mutual Legal Assistance?
+ Subscriber data
+ Traffic data
+ Content data
☐ Other data

22a. If you selected "Other data", please explain the type or category of data:

……..

23. Could you explain the situation for incoming Mutual Legal Assistance requests from third countries? How many requests are received per year? Which are the "top" countries that you receive requests from? What kinds of data are usually requested? Which authorities are involved when processing such a request?

The last 4 years the numbers of the requests for electronic evidence from third countries, received by Bulgarian authorities vary from 2 to 8 per wear. Most of them /5/ are made from USA. There are couple of requests from Turkey.

24. What is the average timeframe for obtaining electronic evidence through Mutual Legal Assistance from your main destination countries outside the EU? Are there any fixed deadlines provided for in your agreement with the countries? Are these deadlines usually respected?

6-12 months

25. When a Mutual Legal Assistance request is refused by a foreign authority, what are the main grounds for refusal (e.g. your main destination country)?

A lack of data and evidence concerning the requested information

26. What are the means of transmission of Mutual Legal Assistance requests to other EU Member States (how you send it)?

+Regular mail (letter)
+ Fax
+Normal email
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other means

26a. If you selected "Other means", please explain:

……

27. What are the means of transmission of Mutual Legal Assistance requests to third countries (how you send it)?

+ Regular mail (letter)
+ Fax
+ Normal email
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other means

27a. If you selected "Other means", please explain:

28. What are the means of transmission of electronic evidence gathered in response to Mutual Legal Assistance requests to other EU Member States (how you receive it)?

+**Regular mail (letter)**
+Fax
+Normal email
+Disks (optical or magnetic)
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other means

28a. If you selected "Other means", please explain:

……

29. What are the means of transmission of electronic evidence in response to Mutual Legal Assistance requests to third countries (how you receive it)?
+**Regular mail (letter)**
+Fax
+Normal email
+Disks (optical or magnetic)
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
☐ Other means

29a. If you selected "Other means", please explain:

……..

3. Jurisdiction in cyberspace / other issues

Part 3 of the questionnaire concerns other measures that law enforcement authorities could use to obtain electronic evidence in cases where:
a) it is not clear that they would stay within their own jurisdiction, e.g. because it is not possible to determine where evidence is stored, or
b) it is clear that they would operate beyond their jurisdiction without using the measures covered under part 1 and 2 of the questionnaire.

30. Can your law enforcement authorities still access electronic evidence when it is unclear what the location of the electronic evidence is / when it is impossible to establish the location of electronic evidence (e.g. when it may be stored beyond your own jurisdiction)?
+ **Yes**
☐ No
☐ It depends on circumstances

30a. If you selected "Yes", or if "It depends on circumstances", please explain how and make reference to the relevant article(s) in your domestic legislation:

When the LEA have permission from the victim or witness to operate with his/her electronic device /computer, mobile phone, etc./, the police officer can access the electronic information wherever its location is.

31. Can your law enforcement authorities still access electronic evidence when it is impossible to obtain electronic evidence that is stored in another country through direct cooperation with a service provider or a request based on Mutual Legal Assistance or Mutual Recognition (e.g. the service provider refuses to cooperate and there is no legal basis for a Mutual Legal Assistance or Mutual Recognition request)?
☐Yes
☐ No
☐ It depends on circumstances

31a. If you selected "Yes" or "It depends on circumstances", please explain how and make reference to the relevant article(s) in your domestic legislation:

32. In the above two situations (see questions 30 and 31), does your domestic law make a distinction between the framework for obtaining access to stored data and the real-time collection of data?
+ Yes
☐ No
☐ Not applicable

32a. If you selected "Yes", please explain how the difference is framed and how this works out in practice:

The access to stored data can be obtained by searches and seizures, interception and seizures of correspondence according art.159-165 Penal Procedure Code.
The real time collection of data is an object of regulation in art.172 Penal Procedure Code /special intelligence means/ and The Special intelligence means Act

the real-time collection of data?

33. To what extent do your authorities use police-to-police cooperation for obtaining cross-border access to electronic evidence? What is the legal framework for such cooperation and what are current practices (e.g. how often, what data, for which purpose)?

Bulgarian LEA very often use police-to-police cooperation for obtaining cross-border access to electronic evidence. The relevant law is the Ministry of Interior Act - art.108-art.119.

34. Is information obtained through police-to-police cooperation admissible as evidence in court in your Member State?
☐ Yes
+ <u>No</u>
☐ It depends on circumstances

34a. If you selected "Not" or "It depends on circumstances", please explain:

Only information obtained by the means of Penal Procedure code can be admissible as evidence in Court and police-to-police cooperation isn't one of them.

[end of the questionnaire]