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

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

Administrative questions

*

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

Romania

*

Please indicate which organisation you are representing

Ministry of Justice

*

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

*

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

- (●) Yes
- ( ) No

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

The Directorate for Investigating Organized Crime and Terrorism Offences, Prosecutor's Office attached to the High Court of Cassation and Justice (Service for Preventing and Combating Cybercrime)

The Romanian National Police (Cybercrime Unit)

Optional inclusion of files

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

```
The answers make reference to:
- Law no. 365/7 June 2002 on electronic commerce
- Emergency Ordinance no. 111/14 December 2011 on electronic communication
(translation not available)

In addition, for the purpose of this questionnaire the following reports
drafted by Cloud Evidence Group (CEG) established by the Cybercrime Convention
Committee (T-CY) might be relevant:

1. Criminal justice access to electronic evidence in the cloud - Informal
summary of issues and options under consideration by the Cloud Evidence Group
available at:
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?document
Id=09000016805a53c8

2. Criminal justice access to data in the cloud: Cooperation with “foreign”
service providers. Background paper prepared by the T-CY Cloud Evidence Group

https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?document
Id=090000168064b77d

3. Criminal justice access to data in the cloud: challenges
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?document
Id=0900001680304b59

CEG will submit to the next T-CY plenary (14-15 November 2016) a draft final
report on Criminal justice access to data in the cloud:  Recommendations for
consideration by the T-CY, as well as a draft Guidance Note to address the
question of production orders for subscriber information under Article 18.
```

Please upload your file(s)

c99867e5-2d59-468f-94ee-2a3a3acaa5a5/LAW___on_electronic_commerce.docx
b4e6d00d-f85a-45a0-a129-5e88f8499074/OUG_111_-_2011.docx

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?

```
Articles 152, 170 and 171 of Criminal Procedure Code
Art.152 – Obtaining data generated or processed by providers of public
electronic communications networks or providers of electronic communication
services intended for the public
ART. 170 – Surrender of objects, documents or computer data
ART. 171 – Forced seizure of objects and documents
```

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)?

```
Yes, there is a separate legal framework for telecommunication services and
providers of information society services, however the procedure for
cooperation is the same.
Information society services providers fall under provisions of article 170
Criminal Procedure Code (see above), the prosecutor ordinance being
sufficient. Providers of public electronic communication networks or providers
of electronic communication services intended for the public (including
telecommunication providers) fall under provisions of article 152 Criminal
Procedure Code) and requires a prior authorization from the Judge for Rights
and Liberties.
Providers of information society services are defined by Law No. 365/2002 on
electronic commerce while the other providers are defined by Emergency
Ordinance No 111/14 December 2011 on electronic communications.
```

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?

```
Considering that such requests are issued within investigations as needed
there are no statistics available.
```

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.

```
Based on penetration of each providers and according to the service provided,
the most relevant providers regarding requests for subscriber information or
traffic data are:
RCS & RDS
UPC Romania
Telekom Romania
Vodafone Romania, Orange Romania are relevant for subscriber information and
phone records
```

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?

- [x] Main seat of the service provider in question
- [ ] Place where services are offered
- [ ] Place where data is stored
- [ ] Other criteria

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:

```
US Facebook, Google
```

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

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

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 covered / allowed

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

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):

The Criminal Procedure Code does not provide definitions for subscriber information, traffic data or content data. However, these concepts are defined in a special law, which implemented the Budapest Convention (Law no 161/2003).

Law No. 161/2003 on measures to ensure transparency in exercising public dignities, public functions and the business environment, preventing and sanctioning corruption, published in the Official Journal of Romania, Part I, No. 279 of 21 April 2003, with subsequent modifications and amendments (Title III – Prevention and combating cybercrime)

Article 35 of Law No. 161/2003
f) data on traffic information means any computer data related to a communication made via a computer system and its products, which is part of the communication chain, indicating the origin, destination, route, time, date, size, volume and duration, and type of service used for communication;
g) data referring to users means any information that may lead to the identification of a user, including type of communication and service used, address, geographical, phone numbers or any other access numbers and manner of payment of that service, and any other data that may lead to identification 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?

- [x] Subscriber data
- [x] Traffic data
- [ ] Content data
- [ ] Other data

11. Do you limit direct requests to cases with specific (e.g. exigent) circumstances or to specific (e.g. serious) crimes?

- ( ) Yes
- (•) No

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?

```
The prosecutor investigating the case.
```

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?

```
Yes, they are sent electronically. They are not tracked. There is no central
repository.
```

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

- ○ Yes
- ◉ No

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?

```
Non EU: Google, Facebook, Skype
No statistics available.
```

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?

```
If reasonable, providers usually respect the deadlines.
```

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

- [ ] Paper (letter)
- [x] Disks (optical or magnetic)
- [ ] Fax
- [x] Normal email
- [x] Web portal
- [ ] Secure channel (encrypted email, special ftp, etc.)
- [ ] Other

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)?

```
However in some situations it depends on other conditions.
```

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?

- [x] Budapest Cybercrime Convention
- [x] Other multilateral conventions
- [x] Bilateral agreements

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

```
Information available in Romanian at:
http://www.just.ro/despre/cooperare-judiciara-internationala-in-materie-penala
/
```

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

```
Information available in Romanian at:
http://www.just.ro/despre/cooperare-judiciara-internationala-in-materie-penala
/
```

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

```
The statistics maintained are not referring to the object of requests other
than the crime investigated.
For cybercrime, top countries are:

EU: UK, Germany, France, Spain
Top third countries: USA, Canada
```

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?

```
The request is initiated by the competent Romanian judicial authority-usually
the prosecutor in charge of the file. The prosecutor after drafting the
request transmits the MLA to the central authority. The central authority
after performing the regularity check is forwarding further the MLA request to
the foreign counter part or is soliciting the completion of the request in
accordance with the applicable legal instrument.

Other authorities involved: General Prosecutor Office, Ministry of Justice and
Eurojust.
```

22. What kind of electronic evidence do you usually request on the basis of Mutual Legal Assistance?

- [x] Subscriber data
- [x] Traffic data
- [x] Content data
- [ ] Other 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?

```
We do not have statistics for incoming MLAT with the object of electronic
evidence.
However, based on the crime investigated (cybercrime) the top countries are:
USA, Germany, UK, France, Spain.
The authorities involved when processing the MLA requests are: Ministry of
Justice, General Prosecutors Office - Directorate for Combating Organised
Crime and Terrorism, Romanian National Police
The data usually requested is: content data, subscriber data, phone records,
interception.
```

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?

```
The timeframe depends from country to country to respond and the importance of
the case.
```

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)?

The foreign authority usually asks for more clarifications if the request is too broad or unclear.

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

- [x] Regular mail (letter)
- [x] 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)?

- [x] Regular mail (letter)
- [x] Fax
- [ ] Normal email
- [ ] Web portal
- [ ] Secure channel (encrypted email, special ftp, etc.)
- [x] Other means

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

Diplomatic channels in case the legal instrument provides so and that particular country has a declaration in this respect.

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)?

- [x] Regular mail (letter)
- [x] Fax
- [x] Normal email
- [x] Disks (optical or magnetic)
- [ ] Web portal
- [ ] Secure channel (encrypted email, special ftp, etc.)
- [ ] Other means

29. What are the means of transmission of electronic evidence in response to Mutual Legal Assistance requests to third countries (how you receive it)?

- [x] Regular mail (letter)
- [x] Fax
- [x] Normal email
- [x] Disks (optical or magnetic)
- [ ] Web portal
- [ ] Secure channel (encrypted email, special ftp, etc.)
- [ ] Other means

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:

The circumstances can refer to the tactical decision to access (or not) the respective data (e.g. risk of being discovered).

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:

The circumstances can refer to the tactical decision to access (or not) the respective data (e.g. risk of being discovered).

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

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)?

```
The authorities in Romania use very often the police-to-police cooperation for
obtaining cross-border access to electronic evidence such as subscriber
information, logs, operative data. The exchange of data can be on a daily
basis.
The legal framework is covered by different laws, bilateral and regional
agreements.
```

34. Is information obtained through police-to-police cooperation admissible as evidence in court in your Member State?

- ○ Yes
- ○ No
- ◉ It depends on circumstances

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

```
some information (ex. minor identifications) can be used in the court if there
is no requirement to be obtained through MLA.
```

Contact

home-cybercrime@ec.europa.eu