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 *

Ministry of Justice of the Republic of Slovenia

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?

-

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?

Direct cooperation between foreign law enforcement authorities and Slovene internet suppliers is not explicitly prescribed in the SI legislation, nor vice versa. Moreover, Slovenia applies the provisions of Council of Europe Convention on Cybercrime (e.g. Article 18), since Slovenia is a signatory of ETS 185.

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)?

As mentioned supra, cooperation requests are not explicitly regulated in the SI legislation. However, the current Art. 149b of our Criminal Procedure Act (ZKP) mentions “operators”. Amendments to this Article that are currently discussed in Slovenia, will in the future add “providers of information society services” therefore a difference will be established.

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?

Slovene Police Department has little experience with these types of requests. In only cca 5 cases court orders were issued by Slovene courts and were subsequently sent (with a translation) electronically to a foreign internet service provider.

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.

The few cases concerned Google, and Facebook.

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:

United States of America.

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 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):

Electronic Communications Act (ZEKom-1) in Article 148 (data on subscribers), Paragraph 1, stipulates:

"(1) Service providers may collect the following data on their subscribers:

1. the personal name of the subscriber or the name of the subscriber's company and its organisational form;
2. the subscriber's address;
3. the subscriber's number or other numbering resources used for the establishment of a connection to the subscriber;
4. if the subscriber so wishes, his academic, scientific or professional title, his website address and other personal contact details (e.g. IM-address) or e-mail address;
5. the tax number for a natural person and the tax and registration numbers for a legal entity;
6. on the basis of payment by the subscriber, additional data, if he so wishes and this does not interfere with the rights of third parties."

Article 3, Point 45 defines:
»Traffic data' shall mean any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.«

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

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

Chapter XIII (Data Retention) of Electronic Communications Act (ZEKom-1) was repealed by our Constitutional Court in 2014 and therefore Slovene operators do not store data as a rule usualy not more than 30 days for commercial purposes.

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?

In most cases Police Department via State Prosecution files a request for a court order to obtain data (data on subscriber, traffic data). State Prosecution sends this request to an Investigative Judge to decide upon it. If a court order is issued it is then translated and send in both language versions electronically to the foreign internet service provider.

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?

Mostly these requests are send electronically. Police Unit in charge of the case monitors these requests and reports back to State Prosecution and Investigative Judge on the results of the court order.

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?

No practice thereof in Slovenia.
See 3a and 3b for partial replies.

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?

As already explained Slovene Police Department has very little experience. In some cases data was obtained within a few weeks time and some requests remained unanswered. Usually no deadline for replying is set.

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:
Not addressed in the SI case law. In our opinion if data is obtained on the basis and in accordance with the Slovene legislation, then it is admissible as evidence in SI courts. .

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:

European Convention on Mutual Assistance in Criminal Matters of 20 April, 1959 with two additional protocols.

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)?

Approximately 30 MLA request are sent to third countries, most of them to the United States. One request was sent to Japan.

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?

A request can be initiated and prepared by a competent Slovenian Court or Prosecutor's Office. They send the request to the Ministry of Justice, who then forwards the request to the competent foreign authority and after receipt of the outcome sends the response back to Slovenian Court or Prosecutor's Office.

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 number of incoming request is much lover then the outgoing. Till now we have received only a few incoming requests. Therefore it is hard to specify the “top countries”. So far the data about IP address was requested. The Ministry of Justice sends the request to the competent Slovenian court for execution and returns the outcome to the requesting country.

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 average timeframe deepens on the type of the information requested. In the first phase, we regularly do receive the notification where the requested authorities (mostly USA) confirm the receipt of the MLA request. In cases of urgency and when the securing of data is requested the response is immediate, however we do face the challenge with receiving the information on content from requested IP. For that the average time can take up to 1 year or more. Sometimes we receive the notification that due to the rule of *“de minimis”* the MLA request could not be complied with.
On the other hand we received the response from the EU member state within 2 weeks from sending the MLA request.
As we mostly use the Cybercrime convention or the principle of reciprocity, there are not any fixed deadlines. The Cybercrime Convention however does in paragraph 7 of Article 27 define that the requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance and that reasons shall be given for any refusal or postponement of the request.
With reference to that, we are of the opinion that it would be of great help if the requested Parties would as far as possible comply with that provision of the Cybercrime Convention.

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)?

Rule of *“de minimis”*. In some cases requests are refused as the records of the internet provider were stored in other country.

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:

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 inpractice:

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)?

Please see next answer

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:

The vast majority of electronic evidence contains personal and other sensitive data of users and third persons linked to users. Also the latest legislative activity is strongly oriented towards preserving the highest level of the fundamental right to respect for private life and the right to the protection of personal data. Collection, storage, processing and use of such data can breach the right to communication privacy which, as said above, is a fundamental human right. With respect to that such data shall be treated in an appropriate manner. According to The Constitution of The Republic of Slovenia, only a law may prescribe that on the basis of a court order the protection of the privacy of correspondence and other means of communication and the inviolability of personal privacy be suspended for a set time where such is necessary for the institution or course of criminal proceedings or for reasons of national security. When dealing with criminal offences such applicable law is the Criminal procedure Act. In our state, the process of obtaining sensitive personal data for the purposes of criminal proceedings is always subject to court surveillance – without a court order, such information obtained only through police to police cooperation is not admissible as evidence in court.

Without prejudice to the above, the court's assessment of the admissibility of the evidence, obtained from abroad, is based on different criteria, when such evidence were collected without cooperation between domestic and foreign authorities (e.g. prior criminal investigation in foreign state which was carried out exclusively for the purposes of that state). In such cases it is clear that our authorities had no impact on how the evidence had been collected. Although the legal standards for collection, storage, processing and use of such evidence can be higher in our state, that does not automatically exclude the evidence as illegally obtained, stored or processed. In such cases our court only assesses whether the evidence was obtained in accordance with the laws of foreign state and in a manner, substantially coherent with our constitutional rules.

[end of the questionnaire]