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

Slovak Republic

* Please indicate which organisation you are representing

Ministry of Justice of the Slovak Republic

* 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?

- General Prosecutors Office of the Slovak Republic
- Ministry of Interior of the Slovak Republic

Optional inclusion of files

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

```
Note - responses are related to the actions taken solely within the scope of
criminal proceedings, thus when the evidence is collected (this is
particularly important for the admissibility of evidence). Responses do not
contain any other acts of police authorities outside criminal proceedings (no
intelligence part is covered). The framework referred to in the questionnaire
contains information on the legislation and practice related to the Slovak
authorities and providers seated in the Slovak Republic. Obtaining of the
evidence from abroad is only possible on the basis of request for mutual
legal assistance.

For the attached files  - Section 116 of Code of Criminal Procedure
```

Please upload your file(s)

0d4725b9-0125-43e6-a920-5c993cb4e7f4/section_116_Code_of_Criminal_Procedure.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?

The legal framework is provided by the Act No. 351/2011 Coll. on Electronic communications, as amended by later regulations (See in particular Section 63 – Telecommunications Secrecy-Subsections 5, 6, 7 and 8) and the Code of Criminal Procedure (in particular Section 116 – communication of telecommunication operations' data and Section 362 of Code of Criminal Procedure – review of proceeding concerning e.g. interception of telecommunication operations and recording of interception communication, etc.). In some cases Section 90 of the Code of Criminal Procedure may be applicable.
For the English version of the Act No. 351/2011 Coll. see http://teleoff.gov.sk/data/files/20551.pdf

Section 90 of Code of Criminal Procedure

Safeguarding and surrendering computer data
(1) If the clarification of facts relevant for criminal proceedings requires to safeguard stored computer data, including operational data saved through the computer system, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings, respectively, may issue an order based on circumstantial reasons to the person who has possession of or control over such data, or to the provider of such services, requesting them to
a) safeguard and maintain integrity of such data,
b) enable making and keeping copies of such data,
c) prevent access to such data,
d) remove such data from the computer system,
e) surrender such data for the purposes of criminal proceedings.
(2) The order referred to in paragraph 1 shall have to specify the period during which the data are to be safeguarded, not exceeding 90 days; a new order shall have to be issued for any extension of that period.
(3) Where there is no longer a need to safeguard computer data, including operational data for the purposes of criminal proceedings, the presiding judge of a panel or a prosecutor prior to the commencement of criminal prosecution or in pre-trial proceedings, respectively, shall issue an order reversing the obligation to safeguard the data.
(4) The order referred to in paragraphs 1 to 3 shall be served on the person who has possession of or control over such data, or on the provider of such services, who may be also imposed the duty to treat the measures set out in the order as confidential.
(5) The person who has possession of or control over computer data shall surrender these data, or the provider of services shall surrender the information that is in his possession or under his control in connection therewith to the authority that issued the order pursuant to paragraph 1.

for Section 116 see the attachment of this questionnaire

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)?

Every person (natural or legal) who wants to do business in the field of networks or services is pursuant to Section 15 of Act no. 351/2011 Coll. on electronic communications required to notify its intention to the Regulatory Authority for Electronic Communications and Postal Services prior to commencement of such service. Such person is also obliged to communicate also changes made in providing network services and their termination. After meeting legal requirements, respective natural or legal persons are covered fully by Act no. 351/2011 Coll. on electronic communications. For this reason our legal framework does not distinguish between providers of internet connection and internet service providers, there is no difference between them (in fact our current legal framework- Act No. 351/2011 Coll. on electronic communications covers only providers of telecommunications services and networks) and for the purposes of cooperation Section 63 (para. 5 - para. 12) of Act no. 351/2011 Coll. on electronic communications may be used.
Cloud providers are not specifically regulated in the Code of Criminal Procedure. The legislation is focused on the type of data (data covered by telecommunication secrecy or data protection rules, including content data). The general framework referred to in respond to question 1 may be applied. With respect to legal framework we need to mention also protection of personal data. As for cloud services we would like to point out to methodological guidance no. 3/2016 of Office for Personal Data Protection of the Slovak Republic which can be accessed at https://dataprotection.gov.sk /uoou/sites/default/files /mu_3_2016_cloudove_sluzby_z_pohladu_zako_na_o_ochrane_osobnych_udajov_pdf.pdf

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?

Unfortunately, such statistics are not being kept by respective authorities. No fresh statistical data is available. However, data has been provided on the basis of a request of the commissioner Malmstrom in relation to the application of the Directive 2006/24/ES in 2012. Moreover, taking into account the impact of the rulings of the Court of Justice of the EU and the Slovak Constitutional Court any fresh data would not provide the real picture, since the system was significantly affected by these rulings.

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.

```
It is difficult to determine since statistics of court orders are not kept.
But we may estimate that “top” services are following:
all major telecommunication providers, such as Slovak Telekom, Orange, O2,
and other providers such as UPC, Slovanet and News and Media Holding.
```

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

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:

Pursuant to Section 63 para. 7 of Act no. 351/2011 Coll. on electronic communications data that are subject of telecommunication secrecy are provided only on the basis of written request and written consent of judge (other data that are not subject of telecommunication secrecy are granted protection on the basis of protection of personal secrecy as stipulated by Act no . 122/2013 Coll on protection of personal secrecy). It follows from the above that for the purposes of obtaining such data by another State it is necessary to request them through mutual legal assistance. Any other possibility is not provided for by law.
In criminal proceedings held in respect of an intentional criminal offence punishable by prison sentence for a maximum period of at least three years, for an offence o of protection of privacy in a habitation; fraud; serious threats; serious stalking; disseminating false news; incitement; condoning a criminal offence, for a criminal offence which caused a grievous bodily injury or death or for other wilful criminal act, as stipulated in international treaty, an warrant to disclose and provide telecommunication data covered by telecommunication secrecy, or subject to protection of personal data, if such data is necessary to clarify the facts relevant for criminal proceedings. A warrant may be issued only if stated purposes cannot be achieved otherwise and if its achievement by other means would be considerably impeded.
We also need to point out to the protection of personal data which is also stipulated in the above mentioned act in Section 56.
For the purposes of Data can only be provided on the basis of the procedures regulated in the Act No. 351/2011 Coll. and Code of Criminal Procedure (in particular Section 116).
According to Section 531 „Procedural acts carried out after the commencement of the criminal proceedings in the Slovak Republic in the territory of another State on the basis of a request by the Slovak authorities or such acts carried out in the territory of the Slovak Republic on the basis of a request by foreign authorities, in particular service of documents, hearing of persons and taking of other evidence, shall be understood as legal assistance.”
According to Section 533 para 1
(1) Slovak authorities shall carry out the legal assistance requested by foreign authorities in the manner provided for in this Code or in an international treaty. If the legal assistance shall be provided on the basis of an international treaty by a procedure not provided for in this Code, the responsible prosecutor shall decide how such assistance shall be carried out.
According to Section 539 para 1
(1) If under this Code the taking of evidence requested by the foreign authority requires a warrant of the court, such warrant shall be issued by a judge upon a motion by the prosecutor responsible for the execution of the request.
In such cases dual criminality is required.
It follows from the above that for the purposes of obtaining such data by another State it is necessary to provide a request for mutual legal assistance. Any other possibility is not provided for by law.

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):

Pursuant to Section 57 para 1 of Act no. 351/2011 Coll. on electronic communications traffic data means any data related to the user and the particular conveyance of information in the network and arising during such a conveyance, which are processed for the purpose of conveyance of a communication in the network or for billing purposes.
As stipulated in para 2 Location data means any data processed in a network or by a service that indicate the geographic location of the terminal of a user of a public service. The undertaking may process location data other than traffic data which relate to a subscriber or user of a public network or public service only if they are made anonymous or with their consent, and in the scope and time necessary for the provision of a value added service. The undertaking shall be obliged to inform the subscriber or user, prior to obtaining its consent on location data other than traffic data which will be processed, on the purpose and duration, and whether the data will be provided to a third party for the purposes of the provision of the value added service. The subscriber or user may revoke its consent for the processing of the location data anytime.
Pursuant to Section 63 para 1 The subject of telecommunications secrecy shall be:
a) The content of conveyed messages,
b) The related data of the communicating parties which are the telephone number, business
name and the place of business of a legal person, or business name and the place of business
of a natural person - undertaker or the personal data of a natural person which are the name,
surname, title and permanent residence address; the data published in the telephone directory
shall not be subject to telecommunications secrecy.
c) Traffic data, and
d) Location data.

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
- [x] Other data

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

Any of listed data on the basis of the warrant of the court (applicable only to providers seated in the SVK).

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?

We need to distinguish between approaches as per Act No. 171/1993 Coll. on Police Force and approach as stipulated in the Code of Criminal Procedure. With respect to the criminal proceedings, if legal conditions are fulfilled, police/investigator notifies prosecutor with the request for ensuring electronic evidence. If prosecutor agrees with this approach he/she requests the court to issue an order (warrant) pursuant to Section 116 of Code of Criminal Procedure. In relation to internet service providers, this approach will be used primarily. Prosecutor may also use approach as stipulated in Section 90 (before the commencement of criminal proceedings and in preparatory proceedings). Court may be requested pursuant to Section 116 of Code of Criminal Proceedings or order may be issued pursuant to Section 90 of Code of Criminal proceedings also without request/input from police officer.

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?

Orders issued in accordance with Section 90 and 116 of Code of Criminal Procedure are sent to service providers in paper form as provided by law (. An order (warrant) issued in specific case is a part of the file.
More information can be found in the Report on Slovakia from the 7th round of Mutual Evalutions (it should be noted that Section 116 of the Code of Criminal Procedure has been amended due to decicision of the Constitutional Court)

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?

This is not applicable.

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?

The question of order handling also depends on several factors (provider, range of requested data, etc.) For this reason it is not possible to provide data on average duration of execution of orders, which would be statistically meaningful. It should be however noted, that usually are orders executed within days, or several weeks respectively. It is also possible to set a time limit for its execution .

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

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

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

```
No evidence is transmitted directly. In crossborder situations  the evidence
is transmitted only through MLA.
```

18. Is information gathered through direct requests admissible as evidence in court in your Member State?

- ( ) Yes
- ( ) No
- (•) It depends on other conditions

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

According to the Code of Criminal procedure there are various conditions that determine the evidential value of information. A general provision on the evidence (Section 119 of the Code of Criminal Procedure) is the leading provision, which provides a general framework for admissibility of evidence. However, when it comes to the evidence obtain from abroad, the rules regulated in Section 531 and in particular 535 have to be followed .

Section 119

General Provisions

(1) In criminal proceedings it is required to prove, in particular

a) whether the act occurred, and whether it has the characteristics of a criminal offence,

b) who committed such act and based on what motives,

c) the seriousness of an act, including the causes and circumstances of its commission,

d) the personal circumstances of the offender to the extent necessary to determine the type and penalty, and the imposition of protective measures and other decisions,

e) the consequences and the amount of damage caused by the criminal offence,

f) proceeds from the criminal activity and the means of its commission, its location, nature, terms and cost.

(2) Anything that might contribute to the proper clarification of the matter and what was gained from the means of proof may serve as evidence under this Act or under a special Act. Means of proof are mainly the interrogation of the accused, witnesses, experts, opinions and expert statement, review of the statements on-site, recognition, reconstructions, investigative experiments, surveys, items and documents relevant to the criminal proceedings, notifications, information obtained through the use of information technology means, or means of operative investigative activities.

(3) The parties may also procure evidence at their own expense. In the case of an acquittal under Section 285 Paragraphs a), b) or c), the State shall reimburse the costs incurred by the accused for this purpose.

(4) Evidence obtained by unlawful coercion or threat of coercion may not be used in the proceedings except when used as evidence against the person that used such coercion or threatened coercion.