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

Austria

*

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?

Optional inclusion of files

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

```
Decree of the Ministry of Justice to which answers to the questionnaire refer
to
Answer to question 18a because the form didn't allow the full answer due to
figure restrictions
```

Please upload your file(s)

20a8f54e-733e-40ab-95a7-1879d84acd05/Answer_to_Question_18a.docx
0a872d37-cc03-4564-a7ed-8154d2080fe4/D__RH-USA_Sicherung_von_Internetdaten_April07.pdf

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?

```
In general, direct cooperation with parties situated outside the territory of
Austria is not allowed. However, only for preservation-purposes the US
Department of Justice has allowed direct contact with service providers
regarding internet-traffic and user data since such data is often stored for a
very short period of time. The Federal Ministry of Justice has informed its
judicial authorities of that circumstance via the decree attached to the
questionnaire which is only available in German language.
Nevertheless it is still necessary to submit an official MLA request in order
to receive the data.
```

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)?

No

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?

No statistical data 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.

facebook, Yahoo, apple, Google

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
- [x] 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:

```
USA (see also answer to question 1)
```

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:

On EU level Art. 48 of Regulation 2016/679/EU provides for:
“Transfers or disclosures not authorised by Union law
Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.”

On national level
Art 10a of the Basic Law of 21 December 1867 on the General Rights of Nationals in the Kingdoms and Länder represented in the Council of the Realm states: “Telecommunications secrecy may not be infringed. [2] Exceptions to the provision of the foregoing paragraph are admissible only by reason of a judicial warrant in conformity with existent laws.“
Additionally, Sec 92 the Telecommunications Act provides for (only available in German language):
„(1) Die Bestimmungen dieses Abschnitts gelten für die Verarbeitung und Übermittlung von personenbezogenen Daten in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen einschließlich öffentlicher Kommunikationsnetze, die Datenerfassungs- und Identifizierungsgeräte unterstützen. Soweit dieses Bundesgesetz nicht anderes bestimmt, sind auf die in diesem Bundesgesetz geregelten Sachverhalte die Bestimmungen des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, anzuwenden. (2) Die Bestimmungen der Strafprozessordnung bleiben durch die Bestimmungen dieses Abschnittes unberührt. […]“

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):

```
Sec 92 para 3 of the Telecommunications Act provides e.g. for the following
3) Irrespective of Article 3, in this section the term [...]
2a.        “subscriber identifier” means an identifier which enables
communication to be attributed unambiguously to a specific subscriber;
3.        “master data” means all personal data required for the
establishment, processing, modification or termination of the legal relations
between the user and the provider or for the production and publication of
subscriber directories,
a) name (surname and first name in the case of natural persons, name or
designation in the case of legal entities);
b) academic degree in the case of natural persons;
c) address (address of residence in the case of natural persons, place of
establishment or billing address in the case of legal entities);
d) subscriber number and other contact information for the message,
e) information about manner and content of the contractual relationship,
f) credit-worthiness;
4.        “traffic data” means any data processed for the purpose of the
conveyance of a communication on a communications network or for the billing
thereof;
4a.        “access data” means the traffic data created at the operator during
access by a subscriber to a public communications network and required for
assignment to the subscriber of the network addresses used for a communication
at a specific point of time;
5.        “content data” means the contents of conveyed communications (No.
7);
6.        “location data” means any data processed in a communications network
or by a communications service, indicating the geographic position of the
telecommunications terminal equipment of a user of a publicly available
communications service; in the case of fixed-link telecommunications terminal
equipment, location data refer to the address of the equipment;
```

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?

Typically in urgent cases to avoid any deletion of the data for a following formal legal request. Initiated by the police, done by the public prosecutor.

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?

By fax or e-mail; Not trough central authority.

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?

See question 3b.

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?

```
No statistics available; No deadline fixed.
```

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.)
- [ ] 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)?

```
See Attachment
```

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:

European Convention on Mutual Assistance in Criminal Matters of 20.04.1959 and its Protocols

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

USA, Australia, Israel, Canada, Supplementary Agreements with Liechtenstein and Suisse, Bosnia Hercegovina, Kosovo

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)?

No statistics available; USA “top”, because the main international providers have their head offices in the U.S.

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?

Requests are made by the prosecution service during the investigation proceedings and by the competent court during the trial phase after an indictment has been filed with the court.
Within the EU direct contacts between the respective authorities of the MS is the rule whereas with regard to third countries requests are submitted via the respective Ministries or even (depending on the respective country) via diplomatic channels.

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
- [x] Other data

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

“location” data, if available and stored. Some providers are denying the storage of “geo” 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?

Requests are transmitted through the Ministry of Justice. No statistics available, Mostly telephone data and telephone records are requested.

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?

No statistics available; No deadline fixed.

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)?

Lack of dual criminality, data not available any more due to deletion; Lack of probable cause required by the law of the requested State, because the link between the data and the suspicion is not sufficiently established under the law of the requested State.

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

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)
- [ ] Fax
- [ ] 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)
- [ ] Fax
- [ ] 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:

Often the location of electronic evidence (e.g. in a cloud) is not known at all or the location changes quickly. Data stored in a cloud or on E-Mail Servers abroad are very often accessible via computers or mobile telephones. In case of a house search or of seizure of hardware (such as mobile phones) all kinds of data can be accessed through this device by law enforcement authorities.

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:

See answer to question 30a.

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:

Please see first answers to question 18a and 30a. Real-time collection of data such as “information about the data of a message transmission” and “surveillance of messages” is regulated under § 134 item 3 and item 4 and § 135 (2) and (3) Code of Criminal Procedure.
Investigative authorities are allowed to access, download and gather data that is accessible from a seized electronic device (e.g. seized in the course of a search of persons or premises) regardless of the location of the server that can be accessed through the device (e.g. cloud-computing or cloud-storage).
The data can be gathered for the purpose of evidence collection, to secure private-law claims or to secure monetary sanctions such as confiscation or forfeiture (§ 110 (1) Code of Criminal Procedure).
Regarding real-time-collection of encrypted data, the Austrian Federal Ministry of Justice is currently preparing legislative measures to implement a new investigative measure for the real-time surveillance of encrypted messages that are being transmitted over a computer system.

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)?

Police to police cooperation is used to explore the requirements for obtaining electronic evidence or if this evidence can be transmitted, because it is already available at the foreign authority. Also used to specify, whether or not the foreign service provider is willing to cooperate with a formal request.

Cooperation between security authorities is regulated by the Police Cooperation Act [Polizeikooparationsgesetz (PolKG)]. Master data can be obtained by the competent security authorities under Art. 5 Par. 3 No. 3 PolKG under specific conditions.
Requests by foreign authorities can be fulfilled by security authorities if the measure would also be possible if a comparable situation arises in Austria.

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

- (●) Yes
- ( ) No
- ( ) It depends on circumstances

Contact

home-cybercrime@ec.europa.eu