# 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

Sweden

*

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?

Swedish Prosecution Authority
Swedish Economic Crime Authority

## Optional inclusion of files

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

Please upload your file(s)

# 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?

```
Traffic data: According to Chapter 6 Section 16a and Section 16d in the
Electronic Communications Act (2003:389), Internet Service Providers (ISPs)
are obliged to store traffic data for six months. (After six months the
information shall be deleted.)

In order to obtain the traffic data for use in preliminary investigation, a
court permission is normally needed and certain requirements must be fulfilled
(see above mentioned Chapter 27 Section 18 and 19 in the Swedish code of
Judicial Procedure).

Subscriber information: According to Chapter 6 Section 16a and Section 16d in
the Electronic Communications Act (2003:389), Internet Service Providers
(ISPs) are obliged to store user information (such as for example name,
address, phone number etc.) for six months. After six months the information
shall be deleted. When suspicions of crime and upon request from prosecution
authority or police authority, the ISP shall give this information to the
requesting authority (Chapter 6 Section 22 (2) in the Electronic
Communications Act). Following the obligation to store the mentioned data for
six months, the request must of course be made within that time.
```

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)?

```
The Electronic Communications Act is applicable to telecommunications
services.
```

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?

```
Since a domestic request is part of the overall investigative tool box and a
request can be made by the prosecutors and the Police across the country,
there is no available, aggregate statistics.
```

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.

See 3a.

## 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
- [x] Place where services are offered
- [ ] Place where data is stored
- [x] Other criteria

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

The key issue is to get access to information for the purpose of bringing an investigation forward. A request may therefore be made according to the Electronic Communications Act domestically or directly to a private party in for instance the US in line with agreed terms of cooperation with the Swedish Police (see 14).

A Internet Service Provider is considered to be domestic if it offers it services within Sweden (see Chapter 2 Section 1 in the Electronic Communications Act (2003:389)).

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 and Canada (STÄMMER DETTA, MIN UPPGIFT)

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):

Direct requests to foreign operators are based on corporate policies on cooperation with law enforcement. In the case of US-enterprises, the US-legislation allows for voluntary disclosure to foreign law enforcement services.

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:

Law enforcement agencies in EU Member States and third countries make requests to the Swedish Police that can obtain the requested subscriber information. For other content data, an MLA is required.

See Chapter 6 Section 20 - 22 in the Electronic Communications Act (2003:389).

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):

```
see 1. A distinction is made between traffic data and subscriber information.


The expression content data is used in Chapter 6 Section 17 in the Act on
Electronic Communication and means information in an electronic communication.
```

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
- [ ] 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 Police Authority and the Prosecution Authority. Some criminal
investigations are run by investigation leaders within the Police. In these
cases, the Police itself initiate a request. In cases where a prosecutor is in
charge of the investigation (typically concerning more serious and complex
offences), the Police make a request on the basis of an instruction from the
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?

As regards requests to foreign service providers, communication van take place via e-mail, but information is channelled through a web-portal. For instance, a request is made to Facebook via a web-portal. An e-mail then confirms that the requested subscriber information is accessible via the web-portal or not.

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?

A particular challenge is that completely domestic, Swedish investigations are hampered by a far too less developed international cooperation as regards accessibility of information and evidence held by private enterprises in a jurisdiction other than the Swedish. It often occurs that a Swedish criminal investigation must be closed due to non-content data not being disclosed from private enterprises in such jurisdictions. The Swedish experience confirms that cooperation with in particular US and US-based corporations are key if we are to succeed in fighting cybercrime. Since it is within the legal powers of these corporations to voluntary disclose non-content data, Sweden has sought to establish agreed ways and procedures of requesting and accessing such information from a number of US-based corporations. In some cases these efforts have been successful. Since 2013, the Swedish Police have, against this background, established a Single Point of Contact (SPOC) in relation to Facebook, Instagram, Ask.fm, Google and Apple. Currently, work is under way to reach a similar agreement with Twitter and Periscope.

Applying the SPOC-concept has many advantages both for the Swedish Police and a private, US counterpart. On the side of the Swedish Police this means that the desk at the Swedish Cyber Crime Centre, the SC3, maintains an overview and gain experience over time on how to manage the cooperation in the best possible way. It also allows for an appropriate supervision of data protection issues. On the side of the private, US counterpart, the use of a SPOC as counterpart allows for smoother processing since becomes an established partner that has provided its necessary credentials for requesting non-content data and receiving voluntary disclosed information.

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 14 A.

In 2015, 490 direct requests were made to the IT-companies mentioned above. At
the end of August 2016, a total of 506 requests have been made. Since the
cooperation for some companies have started only in 2016 there is at present
no baseline for comparison. However, for 2015 Facebook was the service
provider most frequently asked.
```

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 average response time on requests to private companies in the US is
approximately 14 days or less.
```

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

- [ ] Paper (letter)
- [ ] 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)?

There are no admissibility rules for e-evidence, or for any other evidence. The free submission and assessment of evidence is a fundamental principle in the Swedish Code of Judicial Procedure. The procedural system does not contain any formal rules on admissibility and assessment of evidence. Anything that may be of value as evidence in a case may, in principle, be presented in court.

However, evidence obtained from an other state as a result of an MLA request and under the condition that it can´t be used as evidence, is not admissible.

## 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
- [x] Other multilateral conventions
- [x] Bilateral agreements

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

- European Convention on Mutual Assistance in Criminal Matters (with additional protocolls)
- Convention, established by the Council in accordance with Article 34 of the Treaty on European Union, on Mutual Assistance in Criminal Matters between the Member States of the European Union (with additional protocoll)
- Schengen convention

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

Canada, US, Australia and Japan (MLA agreement between EU and Japan)

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)?

There is no statistics on MLA regarding specifically for electronic evidence. However, the total number of requests for mutual legal assistance sent from the Swedish Prosecution Authority during 2015 was 491 (Swedish MLA requests to other Member States: 249, Swedish MLA requests to other Nordic countries: 119, Swedish MLA requests to third countries: 123). The Economic Crime Authority Estimates that they send 2-5 request regarding Electronic evidence / year.

The top country outside EU that Swedish prosecutors send MLA requests to is the USA. In 2015, Turkey was on second place and Canada in third place. The year before, Canada were in second place and Switzerland in third place.

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 prosecutor in charge of the preliminary investigation is also responsible for sending an MLA.
If the request is to be sent to a third country, it will be sent through the Ministry of Justice.

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:

The most common request regards subscriber 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 authority responsible for receiving requests for MLA regarding electronic
evidence is the Swedish Prosecution Authority (SPA). The requests are usually
handled by one of the three International Public Prosecution offices in
Stockholm, Gothenburg and Malmoe. A prosecutor will decide if the request
shall be granted and ask the Police Authority to execute the request.
If the request cannot be granted due to reasons regarding e.g. the crime in
question being a political crime or a military crime, or contrary to
fundamental Swedish judicial rights, the decision to deny legal assistance is
made by the government.

Requests from third countries should be send to the Ministry of Justice.

There is no available statistic on MLAs regarding Electronic evidence.
However, the total number of requests for mutual legal assistance received
during 2015 was 836 (Swedish MLA requests from other Member States: 468,
Swedish MLA requests from other Nordic countries: 244, Swedish MLA requests
from third countries: 124).

The top countries sending MLA requests to Sweden in 2015 are the following.
        Germany (127 requests)        Poland (122 requests)        Norway (88)
The top countries outside EU/the Nordic countries sending MLA requests to
Sweden in 2015 are the following.
        Switzerland (24 requests)          Turkey (22 requests)         USA
(15 requests)

The most requested data is subscriber data, but there are also requests
regarding, traffic data and content data.
```

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?

```
There is no precise statistics available. However, it usually takes a long
time to receive answers. This causes problems due to the Swedish legislation
regarding storage of traffic data; Swedish Internet Service Providers are
obliged to store traffic data for six months and after that time the
information shall be deleted.

According to the Economic Crime Authority it usually takes 6-18 months to
receive an answer from US or Canada.
```

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 main grounds for refusal are that the requested data doesn´t exist – is no longer stored – and (especially with the US and Canada) that the requesting prosecutor hasn´t presented probable cause.

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)
- [ ] 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)
- [ ] 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
- [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)
- [ ] 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

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

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:

```
- In the GENVAL questionnaire earlier this year, Sweden has provided
information regarding access to stored data and the legislation concerning
different kinds of secret coercive measures (real-time).
```

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 question 8 a above.
```

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