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

Belgium

*

Please indicate which organisation you are representing

Belgian Federal Public Service Justice (Ministry of Justice)

*

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

*

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

- (●) Yes
- ( ) No

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

- The cybercrime expertise network of the public prosecutor's office
- The Belgian Federal Police
- The Belgian Federal Public Service Justice

Optional inclusion of files

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

```
- Annex 1 - relevant provisions in the Belgian Code of Criminal Procedure
```

Please upload your file(s)

ffc35e44-6bae-4923-916a-07444134df47/Annex_1_46bis_88bis_90ter.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?

```
Please find in annex 1 the following provisions of the Code of Criminal
Procedure:
-  article 46bis concerning the obtaining of subscriber data;
-  article 88bis concerning the obtaining of traffic data;
-  articles 90ter and 90quater concerning the obtaining of content 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)?

There is in principle no different approach. Articles 46bis, 88bis and 90ter of the Criminal Procedure Code refer to “operators of electronic communication networks and providers of electronic communication services”. Definitions are included in the law on electronic communications of 13/06/2005 (see below).

Definitions in the law on electronic communications:
« réseau de communications électroniques » : les systèmes de transmission, et, le cas échéant, les équipements de commutation ou de routage et les autres ressources, y compris les éléments de réseau qui ne sont pas actifs, qui permettent l'acheminement de signaux par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec commutation de circuits ou de paquets, y compris l'Internet) et mobiles, les systèmes utilisant le réseau électrique, dans la mesure où ils sont utilisés pour la transmission de signaux autres que ceux de radiodiffusion et de télévision; « fourniture d'un réseau de communications électroniques » : la mise en place, l'exploitation, la surveillance ou la mise à disposition d'un réseau de communications électroniques; « service de communications électroniques »: le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission, en ce compris les opérations de commutation et de routage, de signaux sur des réseaux de communications électroniques, à l'exception (a) des services consistant à fournir un contenu (à l'aide de réseaux et de services de communications électroniques) ou à exercer une responsabilité éditoriale sur ce contenu, à l'exception (b) des services de la société de l'information tels que définis à l'article 2 de loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et à l'exception (c) des services de la radiodiffusion y compris la télévision;

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?

```
The Belgian authorities do not dispose of statistics on domestic requests
(there is no single point of contact).
```

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.

```
Whatsapp, Telegram, Skype, Viber, Apple, Snapchat, Twitter, Facebook (incl.
Instagram and Messenger),Yahoo, Microsoft, Google (YouTube, Gmail, 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?

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

5. Do authorities from your Member State make direct requests to service providers in another EU Member State or in third countries?

- (•) Yes, both in EU Member States and third countries
- ( ) Yes, but only in other EU Member States
- ( ) Yes, but only in third countries
- ( ) No, none of the above

5a. If yes, please indicate which third countries (i.e. outside the EU) are most relevant for you in this context:

```
United States
```

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

7a. In case they are mandatory, can and do you enforce them, legally and in practice? Could you please explain how?

Non-compliant service providers, or service providers who refuse to collaborate with the requesting judicial authorities, can be prosecuted on the basis of articles 46bis, §2, 88bis, §4 or 90quater, §2 of the Criminal Procedure Code. The Yahoo-case is a well-known example.

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:

This field was left empty in the original document

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):

```
Article 2 of the law of 13 June 2005 on electronic communication, as amended
by the law of 29 May 2016 on the collection and retention of electronic
communication data:
 6° " donnée de trafic " : toute donnée traitée en vue de l'acheminement d'une
communication par un réseau de communications électroniques ou de la
facturation de ce type de communication;
  7° " donnée de localisation " : toute donnée traitée dans un réseau de
communications électroniques ou par un service de communications électroniques
indiquant la position géographique de l'équipement terminal d'un utilisateur
final d'un service de communications électroniques accessible au public;
```

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
- [x] 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

11a. If yes, please explain:

1. Subscriber data (article 46bis):
The request can be done by a prosecutor or, in cases of extreme urgency, by a judicial police officer for all crimes and misdemeanours. However, if the criminal act cannot be punished with en emprisonment of 1 year or higher, the prosecutor or the judicial police officer can only go back in time 6 months, starting from his request.
2. Traffic data (article 88bis):
The request can be done by an investigating judge when there are serious indications that the criminal act can be punished with an emprisonment of 1 year or higer, and when he thinks that the measure is necessary for the revelation of the truth.
However, in cases of flagrante delicto, the prosecutor can do the request for the criminal acts that are summed up in article 90ter, §2. In §2 of article 88bis, there are further restrictions relating to data that are being held by service providers as a result of the data retention obligation.
3. Content data (article 90ter):
Only an investigating judge can request the interception of content data, and only for the criminal acts that are summed up exclusively in §2 of article 90ter.

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?

A request is usually initiated by the competent judicial authority (investigating judge or prosecutor). He can send his request directly to the service provider, or can go via the intermediary of the Central Technical Interception Facility (CTIF) of the federal police. In practice, it's the CTIF that will carry out the request in cooperation with the 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?

Requests are mostly sent by e-mail, exceptionally by fax or traditional mail. There is no central tracking or repository.

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?

At this moment the Belgian authorities have an agreement with several foreign service providers to obtain identification and localization information.

These agreements are based on a direct communication with these service providers, following the law enforcement guides of these operators.

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?

These requests are either mailed to the service provider or uploaded to a law enforcement portal, managed by this service provider. In 2015 approximately 3500 requests for identification / localization have been made to foreign service providers. For the first 8 months of 2016, 3000 requests have been made. The “top” service providers are Microsoft, Google and Facebook.

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?

```
This depends on the type of crime. A normal request will take approximately 3 weeks to be handled. Whenever an urgent identification / localization is needed (missing persons, terrorism, …) an urgent procedure is used. This indicates that the answer is provided within the same day of the request to the foreign provider.
```

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

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

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

```
This depends on the foreign operator. Certain operators use e-mail to provide the requested information. Other operators will provide an access to a portal website to download the information. All information is received in a digital format.
```

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)?

```
Art. 32 Preliminary title of the Code of Criminal procedure:
La nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si
:
   - le respect des conditions formelles concernées est prescrit à peine de
nullité, ou;
   - l'irrégularité commise a entaché la fiabilité de la preuve, ou;
   - l'usage de la preuve est contraire au droit à un procès équitable.
```

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 + additional
protocols
-  Agreement with the United States on mutual legal assistance
-  Agreement between the European Union and Japan on mutual legal assistance
in criminal matters
```

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

```
Belgian has concluded a number of bilateral agreements on mutual legal
assistance in criminal matters. These instruments do not have any specific
provisions related to electronic evidence, therefore the same regime applies
as for requests for 'traditional' investigative measures.
```

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.

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 public prosecutor or investigating magistrate drafts a request for mutual legal assistance, which he/she sends to the single point of contact in the receiving state as determined in the applicable treaty regarding mutual legal assistance between the requesting and receiving state. For the EU member states e.g. this request can be sent directly to the public prosecutor's office in the receiving state (sometimes via Eurojust). For third (non-EU) countries, this request is mostly 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
- [ ] Other data

23. Could you explain the situation for incoming Mutual Legal Assistance requests from third countries? How many requests are received per year? Which are the "top" countries that you receive requests from? What kinds of data are usually requested? Which authorities are involved when processing such a request?

The requesting authority sends his/her request directly to the district prosecutor's office (for EU-member states) or through the Ministry of Justice (for non-EU third countries). The federal prosecutor's office can serve as a point of entry for any MLA-request which will than be forwarded to the competent district prosecution office. The federal prosecutor will also take on any MLA-request which can not be located within a specific district. The prosecutor subsequently instructs the police with the request or asks the investigating magistrate to do so (e.g. search and seizures, real-time interception of telecommunication, etc.).

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 deadlines are provided for in the agreements.

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 the following:
- double incrimination requirement not met (e.g. slander/defamation vs. First Amendment);
- No probable cause present (proportionality/subsidiarity condition).

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.)
- [x] Other means

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

```
Official diplomatic channels
```

28. What are the means of transmission of electronic evidence gathered in response to Mutual Legal Assistance requests to other EU Member States (how you receive it)?

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

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

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

3. Jurisdiction in cyberspace / other issues

Part 3 of the questionnaire concerns other measures that law enforcement authorities could use to obtain electronic evidence in cases where
a) it is not clear that they would stay within their own jurisdiction, e.g. because it is not possible to determine where evidence is stored, or
b) it is clear that they would operate beyond their jurisdiction without using the measures covered under part 1 and 2 of the questionnaire.

30. Can your law enforcement authorities still access electronic evidence when it is unclear what the location of the electronic evidence is / when it is impossible to establish the location of electronic evidence (e.g. when it may be stored beyond your own jurisdiction)?

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

30a. If you selected "Yes", or if "It depends on circumstances", please explain how and make reference to the relevant article(s) in your domestic legislation:

```
Article 88ter of the Criminal Proceedings Code states that in case the
investigating magistrate orders a search in an IT-system of part thereof, this
search can be expanded to any IT-system or part thereof that is physically
located at a different location if:
-  this expansion is necessary to reveal the truth concerning the crime that
is the object of the search; and
-  if other measures would be disproportionate or if the risk of loss of
evidence exists without such an expansion.

However, the expansion cannot go beyond the IT-system or parts thereof that
are accessible to the person authorized to use the searched IT-system.

Should data retrieved by means of such an expanded search, be physically
located abroad, it can only be copied, not removed or made inaccessible.
Furthermore, the investigating magistrate immediately informs the Ministry of
Justice of the state concerned, if it can be reasonably  identified.
```

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 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:

In the above two situations, article 88ter is only applicable to stored data. The notification obligation foreseen in article 20 of the 2000 MLA-convention (which will be replaced by article 31 of the EIO-directive) is applicable in case of real-time collection of telecommunications without technical assistance of another Member State.

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 for obtaining cross-border access to electronic evidence is not used in Belgium. A request or International Rogatory Commission (both initiated by a magistrate) is necessary.

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:

A request from a magistrate is necessary.

Contact

home-cybercrime@ec.europa.eu