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

Netherlands

* Please indicate which organisation you are representing

Netherlands Ministry of Security and 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

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?

```
The answer to this question provides further insight in the legal framework
in the Netherlands for outgoing direct cooperation requests.

In general the Dutch police uses MLA to issue those orders if the private
companies have their main headquarters in a third state. ISP's residing
abroad can be approached directly to cooperate with requests / orders on a
voluntary basis, with prior consent from the government of the country where
a company resides. The Netherlands has good experiences with this work method
in practice.

In general criminal investigations and prosecution procedures are regulated
in the the Dutch Code of Criminal Procedure (Wetboek van Strafvordering,
DCCP. DCCP has several powers to issue orders for the collection of evidence
by:

- Search and seizure of information system/computer data (general seizure
provisions art. 95, 96, 96a, and 104 DCCP, art. 125i power to search in order
to preserve data, 125j DCCP power to conduct a network serach)

- Preservation of computer data (art. 126ni DCCP)
Art. 126ni DCCP enables the public prosecutor, in cases of crimes for which
pre-trial detention is allowed and which seriously infringe the rule of law,
to order someone to preserve data stored in a computer that are particularly
vulnerable to loss or change. The preservation can be ordered for a period of
at most 90 days (extendible once).

- Order for stored traffic/content data
in January 2006 the Data Production Orders Act (Wet bevoegdheden vorderen
```

gegevens) enacted several powers to order the production of data. The powers were placed in the DCCP. The powers make a distinction of identifying data, other data and sensitive data. The orders can be given to persons who process the data in a professional capacity; an order for “other” stored data and sensitive data can, however, also be directed at persons who process data for personal use.
According to art. 126nc DCCP identifying data can be ordered by an investigating officer in case of a crime (not a misdemeanor). Identifying data are name, address, zip code, date of birth, gender, and administrative numbers.
According to art. 126nd DCCP other data can be ordered by the public prosecutor in cases for which pre-trial detention is allowed. Moreover, future data can also be ordered, including – in urgent cases and with permission of the investigation judge – real-time delivery of future data, for an extendible period of four weeks (art. 126ne DCCP). This enables law enforcement officers to require production of all data that will come into being in future weeks.
According to art. 126nf DCCP sensitive data can be ordered by the investigation judge in case of a pre-trial detention crime that seriously infringes the rule of law. Sensitive data are data relating to religion, race, political or sexual orientation, health, or labor union membership. Stored data at a public telecommunications provider may only be ordered with consent of a judge (art. 126ng, para 2 DCCP).

– order for user information
In order to obtain user data art. 126na DCCP provides for an investigating officer the possibility to order a communications service provider, in case of a crime, to produce user data. User data are name, address, telecommunications number, and type of service. Art. 126n DCCP, concerning traffic data (infra), also comprises the collection of user data. Other information pertaining to the identity of a person may be ordered under art. 126nc DCCP.

• real-time interception/collection of traffic/content data;
Art. 126m DCCP enables the public prosecutor, with authorization from a judge, to order the recording of communications that are generated by means of a communications service provider’s service. Interception is permitted in cases for which pre-trial detention is allowed and which seriously infringe the rule of law. If the intercepted communications turn out to be encrypted, an order to decrypt may be directed at the person who is likely to know the decryption means, but not at the suspect, according to art. 126m para. 6 and 7 DCCP.

–order to make data inaccessible
In the interest of public order or the protection of victims, (e.g, children under 18 that have fallen victim to child sexual abuse of which pictures were made and are disseminated) merely copying the data may not suffice. In those cases article 125o DCCP allows the prosecutor to order an internet service provider to make the data inaccessible. This will be a preliminary situation because the definitive deletion of the data – or their restoration, if the

making inaccessible was unjustified - must be ordered by a judge in court (art. 354 DCCP).

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)?

Not for the investigative powers mentioned above.
Telecommunications providers have, under the Dutch Telecommunications act the obligation to ensure that a network or a facility (used in the supply of a carriage service) has the interception capability to enable a communication passing over that network or facility to be intercepted in accordance with a warrant issued under the TIA Act.

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?

data not 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.

data not available

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

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

The United States of America, Canada

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:

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):

```
- Identifying data: name, address, zip code, date of birth, gender, and
administrative numbers
- Sensitive data: data relating to religion, race, political or sexual
orientation, health, or labour-union membership
- Other 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?

- [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

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?

```
Both public prosecutors and investigating judges are empowered to order a
direct request which will then be handled by the police.
```

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?

These requests are made based on the requirements from the service providers (e-mail, online portal, fax message). These requests are tracked individually by the person who initially made the request. There is no single authority in place which manages a repository of requests.

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?

This information cannot be disclosed without prior consent of the companies concerned.

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?

At the moment the Netherlands Nation wide database concerning MLA request (LURIS) is not designed to retrieve this specific information automatically. Currently discussions on redesigning the LURIS system are started and this ommission will be dealt with during the next release of the upgraded LURIS system.

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?

There is no timeframe other than as soon as possible applicable.

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

- [x] Paper (letter)
- [ ] Disks (optical or magnetic)
- [ ] Fax
- [x] 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

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

Information gathered through direct requests is admissable as evidence in court preferably accompanied with a general consent letter from the government of the country where a company resides.

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

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

```
USA, Canada
```

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)?

```
Numbers are not specified for inside/outside EU

2012: 103
2013: 226
```

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?

In the Netherlands, the administrative handling of all incoming and outgoing requests for mutual legal assistance, both for judicial and police assistance, are organized in 10 International Legal Assistance Centers (Internationale Rechtshulp Centra, IRC) and one National IRC (LIRC) and the Department for International Affairs and Legal Assistance in Criminal Matters (Afdeling Internationale Aangelegenheden en Rechtshulp in Strafzaken) of the Ministry of Security and Justice also forms part of this national network. An IRC is a joint venture between the public prosecutions department and the police.

Both public prosecutors and investigating judges are empowered to issue letters of request.

Under Article 15 of the European Convention on Mutual Assistance in Criminal Matters (in urgent cases), the Benelux Treaty on Extradition and Mutual Assistance in Criminal Matters, and the Convention on the Schengen Agreement, the request can be sent directly from the issuer to the judicial authorities in the state applied to. Where direct transmission is not possible, the public prosecutor and/or the investigating judge passes the request to the Department for International Affairs and Legal Assistance in Criminal Matters at the Ministry of Justice. The Office then sends the request to the foreign authority.

Where no treaty is applicable, the requests are sent solely through diplomatic channels, involving the Ministries of Justice and of Foreign Affairs.

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?

Each district public prosecutor’s office (arrondissementsparket) and all police bodies are linked to one of the IRCs. A request must therefore be sent to the IRC concerned. Where it is not known which pubic prosecutor’s office or which police region is competent, a request for mutual legal assistance may be sent to the LIRC, a joint venture between the National Public Prosecutor’s Office (Landelijk Parket) and the National Police Force which sees to the handling and/or forwarding of the request.

In the absence of a Treaty or Agreement or where direct contact at the level of the public prosecutions department is excluded, the Ministry of Security and Justice (Office for International Affairs and Legal Assistance in Criminal Matters) will continue to act as the central authority to which all requests for mutual assistance in judicial matters must be sent. Where the National Police Agency is designated as the central authority for police requests and no covenants have been concluded concerning the exchange of police information between border regions, the request must be sent to the LIRC which sees to the handling and/or forwarding of the request.

This organization does not affects the competent judicial authorities referred to in the treaties. Requests for mutual legal assistance may be addressed to the competent public prosecutor. Subsequently addressing the request to the right IRC will accelerate the handling of the request.

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?

Anywhere between 2-12 months.

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)?

Mutual legal assistance requests from the Netherlands sometimes fail 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)
- [x] Fax
- [ ] Normal email
- [ ] Web portal
- [x] 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
- [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

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:

```
This would, under strict conditions, be possible under the proposed law,
which will be discussed in the near future in Parliament, Computer Crime III.
After the location of the data is determined, contact and coordination with
the respective Member State on how to proceed is considered the next step.
```

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:

```
This would, under strict conditions, be possible under the proposed law,
shortly being discussed in Parliament. See explenatory report Computer Crime
III.
```

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:

```
This possibility applies to stored data.
```

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 may be possible. If information on data is shared before a formal request for transfer is received, the information may be shared on a police to police basis with the consent of the prosecutor, with the note the information may only be used for investigative purposes. To be able to use the information as evidence in criminal proceedings, the requesting country must send a formal MLA-request for transfer. In some specific cases countries, and the Netherlands as well, send spontaneous information to other states

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:

To be able to use information obtained through police-to-police as evidence in court a formal MLA requests is required.

Contact

home-cybercrime@ec.europa.eu