

## 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

Ireland

\* Please indicate which organisation you are representing

Department of Justice & Equality

\* 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?

Communications (Retention of Data) Act 2011

<http://www.irishstatutebook.ie/eli/2011/act/3/enacted/en/html>

Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993

<http://www.irishstatutebook.ie/eli/1993/act/10/enacted/en/html>

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 Communications (Retention of Data) Act 2011 makes no distinction.

The Interception of Postal Packets and Telecommunications Messages (Regulation) Act 1993 does not cover Information Society Services and is currently being amended to achieve this.

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?

Retained Data under the 2011 Act  
Subscriber Information requests - 10,000 approx.  
Other retained data (time, location, number etc - 10,000 approx.

Requests to intercept communications under the 1993 Act  
This information is confidential

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.

This information is not recorded. All the main service providers in the telecommunications sector are required to provide data, e.g. Vodafone, Eir, Three Ireland, Virgin Media, O2

## 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
- ☐ Place where services are offered
- ☐ Place where data is stored
- ☐ Other criteria

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

- ☐ Yes, both in EU Member States and third countries
- ☐ Yes, but only in other EU Member States
- ☐ Yes, but only in third countries
- ☒ No, none of the above

6. Does your domestic law address such direct requests from your authorities across borders specifically? Or do you apply the same framework as for domestic requests?

- ☒ The same legal framework
- ☐ Regulated specifically

7. Are direct requests sent from your country directly to a service provider in another country considered mandatory or voluntary for the provider to comply with?

- ☐ Mandatory
- ☐ Voluntary

8. Does your domestic law allow service providers established in your Member State to respond to direct requests from law enforcement authorities from another EU Member State 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:

Part 3 of the Criminal Justice (Mutual Assistance) Act 2008  
<http://www.irishstatutebook.ie/eli/2008/act/7/section/22/enacted/en/html#part3>

Replies to questions 8 and 8a refer only to requests for telecommunications interception from the law enforcement authorities of other Member States to the Irish authorities under Part 3 of the Criminal Justice (Mutual Assistance) Act 2008.

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 links to relevant legislation above

The 2011 Act defines a service provider along the lines of the definition used in the EU Data Retention Directive.

The 1993 Act contains no definition of service provider but its scope is limited to telecommunications service providers at this time.

It is important to note that both these Acts are currently under review and definitions may be amended in the near future.

10. What kind of data can be requested directly from service providers according to your domestic law / the law applicable to the service provider?

- ☒ Subscriber data
- ☒ Traffic data
- ☒ Content data
- ☐ 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:

2011 Act

Access to retained data can only be requested for the purposes of the investigation of serious offences, the safeguarding of the security of the State and the saving of human life

1993 Act

Access to content data can only be requested for the purposes of the investigation of serious offences and the safeguarding of the security of the State

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?

2011 Act

Requests for retained data can be made to the service provider by a senior officer of the Police, the Permanent Defence Forces, the revenue commissioners, the Garda Síochána Ombudsman Commission (investigation of police complaints) and the Competition and Consumer Protection Commission

1993 Act

The interception of communications and access to content can only be authorised by the Minister for Justice and Equality.

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 made by Email

Relevant agencies empowered under the Acts maintain their own records.

Department of Justice and Equality also maintains records as required

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?

0 in both cases

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?

Interceptions can be put in place in a matter of hours

The speed at which service provider respond to retained data requests is very much dependent on the service provider.

Response times average from 2 days to a week generally for the majority of providers.

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

- ☐ Paper (letter)
- ☐ 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)?

There are no explicit or implicit articles  
Retained data that has been access under the 2011 can be used in evidence and has been.  
It is the policy of this State not to use content data in evidence. However there is nothing in legislation to preclude doing so.

## 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
- ☒ Other multilateral conventions
- ☐ Bilateral agreements



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

EU and Council of Europe mutual assistance conventions

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)?

In 2015, 90 of 250 requests approx. were transmitted to third countries. 77 requests issued to the United States of America.

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 Prosecution Service makes the request on behalf of the Police Service; the request is transmitted by the central authority for mutual legal assistance which is located within the Ministry of Justice.

22. What kind of electronic evidence do you usually request on the basis of Mutual Legal Assistance?

- ☐ Subscriber data
- ☒ Traffic data
- ☒ 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?

In 2015, 90 of 665 requests approx. were received from third countries. The 'top' third country is Turkey (40 requests) followed by Switzerland (15). Incoming requests are executed by the central authority for mutual legal assistance (Ministry of Justice). A typical request for specified evidential material requires an application to be made to the District Court for a production order.

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?

Requests for electronic evidence are received from the USA within 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)?

Refusals are not common but may arise due to First Amendment issues (free speech) insofar as requests to the US are concerned.

26. What are the means of transmission of Mutual Legal Assistance requests to other EU Member States (how you send it)?

- ☒ Regular mail (letter)
- ☐ Fax
- ☐ 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)?

- ☒ Regular mail (letter)
- ☐ Fax
- ☐ 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)?

- ☒ Regular mail (letter)
- ☐ Fax
- ☐ Normal email
- ☐ 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)?

- ☒ Regular mail (letter)
- ☐ Fax
- ☐ Normal email
- ☐ 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

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)?

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

---