

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 cyberspace¹

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

¹ The electronic version of the questionnaire is available at: <https://ec.europa.eu/eusurvey/runner/eevidence>

Administrative questions

I. Please indicate on behalf of which EU Member State you are responding to the questionnaire*

- ☐ Austria
- ☐ Belgium
- ☐ Bulgaria
- ☐ Croatia
- ☐ Cyprus
- ☐ Czech Republic
- ☐ Denmark
- ☐ Estonia
- ☐ Finland
- ☐ France
- ☐ Germany
- ☐ Greece
- ☐ Hungary
- ☐ Ireland
- ☐ Italy
- ☐ Latvia
- ☐ Lithuania
- ☒ **Luxembourg**
- ☐ Malta
- ☐ Netherlands
- ☐ Poland
- ☐ Portugal
- ☐ Romania
- ☐ Slovak Republic
- ☐ Slovenia
- ☐ Spain
- ☐ Sweden
- ☐ United Kingdom

II. Please indicate which organisation you are representing *

Prosecution Office Luxembourg

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

**Parquet de Luxembourg
Bâtiment PL
Cité judiciaire
L-2080 – Luxembourg
Téléphone : +352 47 59 81 – 438/443**

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

- ☒ **Yes**
- ☐ No

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

General Prosecution Office

Optional inclusion of files

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

N/A.

All the legal provisions specified here below are freely available on the internet sites mentioned in reference and in particular on <http://legilux.public.lu/>.

Va. Please upload your file(s)

[please use the EU Survey website (<https://ec.europa.eu/eusurvey/runner/eevidence>)]

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?

1. In the act/ "in flagrante delicto": Articles 31 and subsequent of the [Criminal Procedure Code](#) (here below referred as "CPC")

2. In case of preliminary investigations: - Articles 24-1, 66 and subsequent, 88-1 and 88-2 of the CPC (domestic investigation orders of an instructional Judge)

- Article 48-25 of the CPC (quick freeze)

- Articles 47 and 33 of the CPC (on a

voluntary base)

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, there is not.

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?

Currently such record is 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.

National telecommunication providers: Orange, Join, Tango and Post Telecom.

Providers of information / society services: Skype, Microsoft, I-Tunes, Amazon, PayPal, Facebook and Ebay.

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

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

N/A

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

X 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:

It is rather an exception and results from best practice: in case of Microsoft we send the domestic order directly to the intermediary company in Luxembourg, in case of Facebook we use the platform from Facebook Inc. to upload domestic investigation orders. Furthermore, we use the Global legal international compliance procedures of the providers in urgency cases.

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?

X The same legal framework

- ☐ Regulated specifically

6a. If regulated specifically, please copy or reference the relevant article(s):

N/A.

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
X Voluntary

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

N/A.

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
X No, this is not covered

8a. Please copy or reference the relevant article(s) providing for the legal basis to allow / prohibit service providers to do so:

N/A

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):

N/A.

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

10a. If you selected "Other data", please explain which type or category of data:

N/A.

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:

N/A.

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 Prosecution Service requests a domestic investigation order from the examining judge.

The issued order is transmitted, executed and notified by the Police Department to 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?

An order issued by an examining judge is always part of a case under investigation. The orders are centralized by the examining judge in the relevant file. Domestic orders are notified on place by the investigating police unit which keeps track of it too.

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?

N/A.

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?

N/A.

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?

Difference has to be made between urgent and non-urgent requests. In urgent matters a result can be obtained within hours. There is no specific timeframe in which a request has to be executed as it always depends on the amount of data requested.

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

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

Business documents are seized on paper meanwhile data is either seized on hard disk or CD-ROM, depending on the volume. In special cases, like the surveillance of chat channels, the data is transmitted through secure channels.

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)?

Evidence gathered in accordance with the provisions set out under answer 1 above may be used in Court.

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

N/A.

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:

- Convention of Mutual Legal Assistance in Criminal Matters dated 20 April 1959
- Convention implementing the Schengen Agreement of 14 June 1985
- Mutual legal assistance convention in criminal matters between de Member States of the European Union dated 29 May 2000

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

- Mutual Legal Assistance Treaty in criminal matters between Luxembourg and the United States of America dated 13 March 1997
- Mutual Legal Assistance Treaty in criminal matters between Luxembourg and Australia dated 24 October 1988
Mutual Legal Assistance Agreement in criminal matters between the European Union and Japan

20. How many Mutual Legal Assistance requests for electronic evidence to third countries are made by your authorities per year? Which are the "top" third countries that you send requests to (outside the EU)?

There are no figures available for outgoing MLA requests.

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 requests the examining Judge to issue a mutual legal assistance request which is transmitted to the General Prosecutor's Office.
The request is then transferred to the central authority of the concerned third country for execution. The request may be sent directly by the examining judge to the foreign executing authority if an international agreement provides for such possibility.

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

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

N/A.

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?

Incoming Mutual Legal Assistance requests amount to more than 700 per year (811 request in 2016) in all criminal matters of which more than 200 are requests in matters of cybercrime. The top countries that Luxembourg receives requests from are (figures for 2016): Germany (215), Belgium (123), France (92), the Netherlands (55) and Switzerland (40) for request in all criminal matters and Germany (102), Poland (18), the Netherlands (15), Ireland (12), Spain (11) for requests in matters of cybercrime. The requests mainly concern the following providers: I-Tunes, Skype, Paypal, Amazon and Ebay. The data requested concerns mainly identification of internet account holders and of IP-address holders.

The local authorities involved in the execution of the MLA requests are: the General Prosecution office (which is the central authority for incoming requests), the Prosecution office of the District Court where the execution of the request is supposed to take place (Luxembourg or Diekirch District Court), the examining judge of the relevant District Court, a police unit executing the request (most requests are executed by a specialized central police unit) and a specialized chamber within the District Court (made up of three judges) which needs to allow the transfer of the seized evidence to the requesting authority.

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?

N/A

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)?

N/A

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:

N/A.

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

X Web portal

☐ Secure channel (encrypted email, special ftp, etc.)

☐ Other means

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

N/A.

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 (in cases of urgency)

X Disks (optical or magnetic)

☐ Web portal

☐ Secure channel (encrypted email, special ftp, etc.)

X Other means

28a. If you selected "Other means", please explain:

Voluminous evidence is frequently collected (especially for neighbouring countries) directly by a police unit delegated by the requesting authority.

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

29a. If you selected "Other means", please explain:

N/A.

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

X 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:

As stated above, in case of Microsoft a domestic order is directly sent to the intermediary company in Luxembourg without regard of the location of the data.

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

X 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:

N/A.

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

X Not applicable

32a. If you selected "Yes", please explain how the difference is framed and how this works out in practice:

N/A.

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)?

Electronic evidence in other countries can only be acquired through MLAT procedures. There is no case known where such data was directly accessible through police-to-police cooperation.

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

☐ Yes

☐ No

X It depends on circumstances

34a. If you selected "Not" or "It depends on circumstances", please explain:

It may not be admissible in case the information was provided upon request by a national police unit in a matter where the request would have to be made by a judicial authority according to relevant MLA law or treaties.

[end of the questionnaire]