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[1]

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 *

Ministry of the Interior of the Republic of Latvia

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

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?

Ministry of the Justice, State Police, General Prosecutor's Office.

Optional inclusion of files

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

Answers to the Questionnaire of 7th round of Mutual Evaluations "*The practical implementation and operation of European policies on prevention and combating Cybercrime*" (hereinafter - Questionnaire of 7th round of Mutual Evaluations).

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?

Legal Framework:

- **Electronic Communication Law** (hereinafter - ECL);
- **Cabinet Regulation No. 820** "*Procedures by which Pre-trial Investigative Institutions, Bodies Performing Investigatory Operations, State Security Institutions, Office of the Prosecutor and Court Request and a Merchant of Electronic Communications Transfers Data to be Retained, and Procedures by which Statistical Information regarding Requests of Data to be Retained and Issuing thereof is Compiled*" (hereinafter - Cabinet Regulation No. 820);
- **Criminal Procedure Law** (hereinafter - CPL);
- **Investigatory Operations Law** (hereinafter - IOL).

More detailed information:

According to the **ECL** Section 1 (8) **electronic communications merchant** is a merchant or a branch of a foreign merchant who has the right to perform commercial activity, to ensure a public electronic communications network[2] or provide electronic communications services[3] in accordance with the procedures laid down in this Law. Furthermore, according to ECL Section 1 (10) **electronic communications service provider** is an electronic communications merchant who provides publicly accessible electronic communications services[4], utilising the public electronic communications network.

[2] **Electronic communications network** is transmission systems, switching and routing equipment (including network elements which are not being used) and other resources, which irrespective of the type of transmitted information permits the transmission of signals utilising wires, radio waves, optical or other electromagnetic means in networks, including:
a) satellite networks, fixed networks (channel and packet switching networks, including Internet) and mobile terrestrial electronic communications networks,
b) networks, which are utilised for radio and television signal distribution,
c) cable television and cable radio networks, electricity cables systems to the extent that they are utilised in order to transmit signals (According to ECL Section 1., 11))

[3] **Electronic communications service** is a service that is usually ensured for remuneration and which wholly or mainly consists of the transmission of signals in electronic communications networks (ECL Section 1. 9))

It should also be noted that electronic communications merchants and electronic communications service providers are **registered** in a dedicated Register (managed by the Public Utilities Commission[5]).

Furthermore, according to the ECL Section 71.[1] (*Utilisation and Processing of Data to be Retained*), the **electronic communications merchants and electronic communications service providers** have the following **duties**, namely, they shall ensure:

- **retention[6] of retained data in such volume as they are acquired or processed in providing electronic communications services**, as well as ensuring the protection thereof against accidental or unlawful destruction, loss or modification, or processing or disclosure not provided for in this Law (it is, however, also stated that the electronic communications merchant does not have a duty to perform additional measures to acquire the data to be retained if in providing electronic communications services, the technical equipment of the merchant does not generate, process and register such data);

- **transfer of the retained data to a number of institutions** [7] on the basis of their request.

Based on ECL Section 71.[1] (4), the government has adopted **Cabinet Regulation No. 820** determining the procedure for both the requesting and transferring of data to be retained to these institutions.

Hence, direct cooperation under the terms of ECL and Cabinet Regulation No. 820 between the law enforcement authorities and the electronic communications merchants/ electronic communications service providers is mandatory only if they are registered with accordance to ECL.

However, there are **other private sector entities** who are **also providing electronic communication services** but are not registered with accordance to ECL[8] **(hereinafter – "entities providing electronic communication services[9]")**.
In such cases these entities are considered as a legal persons and registered in the Enterprise Register) to whom the Criminal Procedure Law (Section 190.-192[10], hereinafter - CPL) and Investigatory Operations Law apply if direct cooperation is needed (hence, for these entities terms of ECL and Cabinet Regulation No. 820 doesn't apply).

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.

[5] Regulator is institutionally and functionally independent, full-fledged, autonomous body governed by public law which carries out regulation of public services in energy, electronic communications, post, municipal waste management and water management sectors.
[6] According to the ECL Section 19 (1) 11 electronic communications merchant and electronic communications service provider has a duty to ensure the storage of data to be retained for 18 months
[7] Pre-trial investigation institutions, persons performing investigative field work, State security institutions, the Office of the Public Prosecutor and the courts (…)
[8] No legal obligations under the national legislation
[9] i.e., social media network "Draugiem.lv".
[10] CPL Section 190 "Submission of Objects and Documents Requested by a Person Directing the Proceedings"; CPL Section 191 "Storage of Data located in an Electronic Information System"; CPL Section 192 "Disclosure and Issue of Data Stored in an Electronic Information System"

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?

In 2015 there were **in total 58 595** domestic requests[11] made to the electronic communications merchants and electronic communications service providers for direct cooperation from the law enforcement authorities[12] (legal basis: Cabinet Regulation No. 820). In more detail:
- requests with regard to the services of the public fixed telephone network – **632**;
- requests with regard to the services of the public mobile telephone network – **50 116**;
- requests with regard to the internet access services – **7847**.

Moreover, in 2015 there have also been approximately **25 102** domestic requests to the "entities providing electronic communication services" for direct cooperation according to the CPL and approximately **15 141** requests according to the Investigatory Operations Law[13].

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.

"Top" service providers" (registered as an electronic communications merchants providing fixed telephone networks, public mobile telephone networks and internet access):
1. Tele2;
2. LMT;
3. BITE Latvia;
4. Lattelecom;
5. Baltcom TV.

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

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?

● 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

[11] Statistics gathered by the Data State Inspectorate according to Cabinet Regulation No. 820 (Section 12)
[12] Includes pre-trial investigative institutions, bodies performing investigatory operations, state security institutions, office of the prosecutor and courts according to Cabinet Regulation No. 820
[13] Statistics provided by the State Police

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

USA (E-Bay, Facebook).

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):

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
● 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 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:

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):

The ECL distinguishes the following types of data: - **subscriber directory** – a structured, ordered compilation of personal data in which by utilising specific attributes it is possible to find information regarding the relevant electronic communications merchant subscriber; - **location data** – data, which is processed in an electronic communications network or processed using electronic communications services and indicates the location of the

terminal equipment of an electronic communications service user. For public mobile electronic communications networks, satellite networks and non-wire networks, which are utilised for the distribution of radio or television signals, it shall be the geographic location (address) of the terminal equipment of an electronic communications service user, but for public fixed networks, cable television and cable radio networks, and electricity cable systems to the extent that they are utilised in order to transmit electronic communications signals – the termination point address;
- **traffic data** – any information or data, which is processed in order to transmit information by an electronic communications network or to prepare accounts and register payments, except the content of transmitted information;
See also answer 2.B.3 to the Questionnaire of 7th round of Mutual Evaluations.

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?

With regard to the law enforcement:

For direct requests, there is a **single point of contacts designated at the State Police** (*Information Bureau of the Central Criminal Police Department*) which is **in charge of requesting and receiving necessary data from** Latvian electronic communications merchants, electronic communications service providers and "entities providing electronic communication services" (on voluntary basis). The single point of contact is available 24/7 and receives requests from all the State Police entities (in each region a contact person is designated).

For direct requests outside Latvia, there is a **single point of contact designated at the State Police** (*International Cooperation Bureau of the Central Criminal Police department*) which is **responsible for international cooperation and information exchange** (it is also designated as a single point of contact under the Budapest Convention).

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?

In both cases requests are made in an electronic form and sent for coordination through the relevant single contact point designated by the State Police (namely, either through the *Information Bureau of the Central Criminal Police Department* or *International Cooperation Bureau of the Central Criminal Police department)*.

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?

For requests going beyond the domestic jurisdiction the Budapest Convention, Mutual Legal Assistance instruments and bilateral agreements apply.

Statistics (number of requests) is not available.

Top service providers – Yahoo.com; Gmail.com; PayPal (USA); Ebay (USA).

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 are no fixed deadlines; they are determined by the law enforcement on case-by-case basis (the service providers though are not always respecting the set deadlines).

The average timeframe to obtain data from service providers through direct requests is approximately two weeks.

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:

n/a

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)?

n/a

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

If information, gathered through direct requests, after its examination is to be considered as evidence, an additional request is sent in order to ensure the admissibility (by using the relevant mutual legal assistance instruments).

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:

European Union Convention on Mutual Assistance in Criminal Matters.

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

Please, see answer 7.A.3 to the Questionnaire of 7th round of Mutual Evaluations.

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)?

Please, see answer 7.A.3 to the Questionnaire of 7th round of Mutual Evaluations.

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?

Mutual Legal Assistance request to a third country are mostly sent by the State Police (through a designated point within the *International Cooperation Bureau of the Central Criminal Police department*) and the Prosecutor's Office.

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

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?

According to the Criminal Procedure Law (Article "*846 Competent Authorities in Examination of a Request of a Foreign State*"):

- in the pre-trial proceedings: the General Prosecutor's Office examines and decides a request of a foreign state; up to the commencement of criminal prosecution also the State Police;
- after transfer of a case to a court: the Ministry of Justice examines and decides a request of a foreign state.

Most often requested data - subscriber and content data.
Top countries – USA, Germany.

Please, see also answer 7.A.3 to the Questionnaire of 7th round of Mutual Evaluations.

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?

Such statistics is not available. There are also no fixed deadlines in the current bilateral 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)?

n/a

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[14]
- ● Normal email[15]
- ☐ 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)?

- ● Regular mail (letter)
- ● Fax[16]
- ● Normal email[17]
- ☐ Web portal
- ☐ Secure channel (encrypted email, special ftp, etc.)
- ☐ Other means

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

[14] Original must be sent afterwards also through the regular post
[15] Original must be sent afterwards also through the regular post
[16] Original must be sent afterwards also through the regular post
[17] Original must be sent afterwards also through the regular post

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)?

- ● Regular mail (letter)
- ● Fax[18]
- ● Normal email[19]
- ☐ Disks (optical or magnetic)
- ☐ Web portal
- ☐ Secure channel (encrypted email, special ftp, etc.)
- ☐ Other means

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

n/a

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[20]
- ● Normal email[21]
- ☐ 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

[18] Original must be sent afterwards also through the regular post
[19] Original must be sent afterwards also through the regular post
[20] Original must be sent afterwards also through the regular post
[21] Original must be sent afterwards also through the regular post

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:

n/a

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:

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
☐ 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)?

Legal framework:

Police-to-police cooperation is carried out in accordance with the Swedish Framework Decision[22] and the Budapest Convention, namely through the single point of contacts established within the *International Cooperation Bureau of the Central Criminal Police department* (which also carries out functions of the cybercrime 24/7 contact point in line with the Budapest Convention and Directive 2013/40/EU).

Current practices:

During the pre-trial investigations, the possibilities provided by Interpol, Europol and Eurojust, including the JITs, are explored.

Mostly information on the subscriber data is exchanged.

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:

If the evidence has been gathered by using the mutual legal assistance instruments they are considered as admissible at the court.

However, if the evidence is gathered on the "*police-to-police*" basis (i.e., through Interpol, Europol channel or by using the Swedish Framework Decision), it is not admissible until the consent of the Member State that provided the information or intelligence has been obtained. Such consent is not required where the requested Member State has already given its prior consent (when transmitting the information or intelligence.

[end of the questionnaire]

[22] Council Framework Decision (2006/960/JHA) of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union