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 *

The Danish Ministry of Justice

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? *

X Yes
☐ No

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

The Danish Ministry of Justice
The Danish National Police, National Cyber Crime Center
The Danish Prosecution Service

Optional inclusion of files

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

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?

The Administration of Justice Act Section 786 a.
(1) In connection with an investigation in which electronic evidence may be of importance, the police may impose orders on providers of telecom networks or services to arrange for emergency protection of electronic data, including traffic data.
(2) An order of emergency protection under subsection (1) above may solely comprise electronic data stored at the point in time when the order is imposed. The order must state the data that must be secured and the period for which they must be secured (the period of protection). The order must be limited to comprise solely the data estimated to be necessary for investigation and the protection period must be as short as possible and no more than 90 days. An order of this nature may not be extended.
(3) Providers of telecom networks or services are responsible for ensuring as part of the protection under subsection (1) without undue delay that they pass on traffic data concerning other telecom network or service providers whose networks or services have been used in connection with the electronic communication that may be of importance for the investigation.
(4) Violation of subsections (1) and (3) above is punishable by a fine.

The Administration of Justice Act Section 804.
(1) *In connection with the investigation of an offence which is subject to public prosecution or a case of violation of an order as referred to in section 2(1) para. 1 of the Act on Restraining, Exclusion and Removal Orders, a person who is not a suspect may be ordered to produce or hand over objects (discovery), if there is reason to presume that an object of which that person has the disposal may serve as evidence, should be confiscated or, by the offence, has been procured from someone who is entitled to claim it back. When an order is imposed on a business enterprise, section 189 shall apply correspondingly to others who have gained insight into the case due to their association with the enterprise.*
(2) *If an object has been handed over to the police following an order of discovery, the rules of seizure according to section 803(1) shall apply correspondingly.*
(3) *If, without any order to this effect, an object has been handed over to the police for the reasons mentioned in subsection (1) above, section 807(5) shall apply. If a request for return of an object is made, and the police do not grant the request, the police shall as soon as possible and within 24 hours submit the case to the court with a request for a seizure order. In that case section 806(4), 2nd sentence, and subsection (6) 1st sentence, shall apply.*
(4) *An order of discovery may not be issued if it will produce information on matters about which the individual would be exempted from testifying as a witness according to sections 169-172.*

(5) *The Minister of Justice may issue rules on financial compensation in special cases for costs relating to the fulfilment of an order for discovery."*

Danish law differentiates between static and dynamic IP-addresses:
- An telecommunications providers *is obligated to produce information that can identify the user of a static IP-address without a court order*
- An telecommunications providers *is obligated to produce information that can identify a user of a dynamic IP-address only in accordance with a court order as stated above*

Interception of telecommunications (content data) etc. is also available according to Section 781 to the serious offences punishable with at least six years of imprisonment if there are reasonable grounds to presume that information is used or being passed from a suspect and that the interception is presumed to be of essential importance to the investigation. This measure includes disclosure of email-correspondence and other available content. This Section concerns tapping communication through the service provider's facilities.

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

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 a total of 6.576 requests for information in accordance with section 781 was made to the Danish telecommunications providers. This number does not include requests made by the Danish Security and Intelligence Service.

There are no available statistical data regarding request for emergency protection of electronic data (section 786 a) or production requests (section 804).

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.

The five largest Danish Telecommunications providers handle the most requests. These are:
- TDC
- Telia
- Hi3G
- Telenor
- Stofa

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:

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:

USA

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):

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?

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 is not specifically regulated but follows from the principle of territoriality.

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)?
X Yes
☐ No

9a. If yes, please provide us with the definition(s):

Subscriber data are covered by The Administration of Justice Act, chapter 74 “Seizure and disclosure”. Section 804 states that as part of an investigation of an offence, which is subject to prosecution by the State, a person, who is not a suspect, can be ordered to disclosure. There must be a reason to presume that the object can serve as evidence, should be confiscated or has been purloined from somebody, who can claim it back.

Traffic data and content data are covered by The Administration of Justice Act, chapter 71 “Invasions of the secrecy of communication, observation and data copying”. Section 780 (1) (1) and (3) states that pursuant to the rules of the mentioned chapter, the police can invade the secrecy of communication by intercepting telephone conversations or other similar telecommunication, and obtain information about which telephones or other similar communication devices are connected with certain telephone or other communication devices.

Those invasions of the secrecy of communication may only be conducted if there are specific reasons to presume that messages are given or mail is delivered by the means in question to or from a suspect, and the invasion is presumed to be of crucial importance to the investigation and the investigation concerns an offence, which under the law can be punished with imprisonment for six years or more.

Disclosure has a much lower degree of probable cause and is therefore applicable in many more investigations. Requests for subscriber data and content data have the same degree of probable cause, which is more intense than disclosure.

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
X Other data

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

Data can only be requested from service providers with a court order, unless the owner of the device consents to the data being provided, cf. The Administration of Justice Act, Section 786 (2).

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:

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 typical request is initiated by the Danish Police and then processed through the Danish Prosecution which then – if the situation requires it (see answer 1) – presents the case to the courts in order to get the relevant court order.

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 sent to the telecommunications providers via a web portal.

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?

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?

There is no statistical data available in this regard.

Direct requests to foreign providers follow the procedure described in answer 12. The request however is then forwarded to the relevant provider typically via the providers online portal (Facebook, Google etc.)

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?

A request to a Danish telecommunications provider is typically expedited within one hour.

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:

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)?

Danish courts use what is called a “free assessment of evidence”. This means that evidence that is brought before a court of law can be used if the court sees fit. The court however is free to weigh how much of an impact on a case a particular piece of evidence will have.

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

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:

The 1959 Council of Europe Convention on Mutual Legal Assistance (or the principles of hereof) and its 1978 and 2001 Additional Protocols (with regards to third countries that haven't signed the Budapest Cybercrime Convention)

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

Hong Kong Special Administrative Region of the People's Republic of China

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 note that the Ministry of Justice per 1 March 2016 has appointed the Office of Public Prosecutions as a central authority regarding mutual assistance in criminal matters.

Because cases regarding mutual legal assistance is a new area of practice for us, we do not have detailed statistics yet.

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 Police Commissioners or State Prosecutors send the request for Mutual Legal Assistance to the Office of the Director of Public Prosecutions, who sends the request to the Ministry of Foreign Affairs. The Ministry forwards the request to the competent authority in the third country, via diplomatic channels. In urgent cases, the request may also be sent via the secure communication channels of Interpol.

22. What kind of electronic evidence do you usually request on the basis of Mutual Legal Assistance?
☐ Subscriber data
☐ Traffic data
☐ Content data
X Other data

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

It is not often we request electronic evidence, but in the cases from the last 6 months, we have requested traffic data and content data a few times.

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?

Please note that the Ministry of Justice per 1 March 2016 has appointed the Office of Public Prosecutions as central authority regarding mutual assistance in criminal matters.

Incoming Mutual Legal Assistance requests from third countries are sent to the Office of the Director of Public Prosecutors.

The request will be sent to the District Police Commissioners, who will provide the requested information and send it back to the Office of the Director of Public Prosecutions, who then sends the information gathered to the requesting country.

The following information is based on cases from 1 March 2016 and forward.
We have received about 150 requests from third countries within the last 6 months.
Many of those are from Switzerland and Turkey. None of these requests regard electronic evidence.

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?

Due to the fact that the Office of the Director of Public Prosecutions only has dealt with Mutual Legal Assistance in about six months, we do not have statistics yet. In those cases we have completed, the cases have been processed with the pace required by the seriousness of the case.

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 reason for refusal is often difference in the use of probable cause. Usually other countries demand a higher degree of probable cause than is needed in Danish law.

26. What are the means of transmission of Mutual Legal Assistance requests to other EU Member States (how you send it)?
☐ Regular mail (letter)
X Fax
X Normal email
☐ Web portal
☐ Secure channel (encrypted email, special ftp, etc.)
X Other means

26a. If you selected "Other means", please explain:

We usually send via regular mail or fax. We would very much like to use secure channels (encrypted email), but that is often only possible for Interpol to do so.

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
☐ Normal email
☐ Web portal
X Secure channel (encrypted email, special ftp, etc.)
X Other means

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

We send by letter or fax, or via secure channels through Interpol. Alternatively eg. FedEx may be used in urgent matters.

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

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

FedEx

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

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

FedEx

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:

On 10 May 2012, the Danish Supreme Court delivered a decision in a case regarding data acquisition of a Facebook and a Messenger profile belonging to a suspect in a criminal investigation. The Supreme Court decided that the Danish Police were allowed to gain access to the Facebook and the Messenger profiles via the internet using the correct codes for the profiles that had been obtained through other investigative measures. The reasoning behind this was that the crime that was being investigated was subject to Danish criminal jurisdiction and that access to the profiles could be achieved via the internet without having to involve foreign authorities.

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 answer 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:

No clear judgement has been made at this time so it isn't possible to say.

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)?

The National Cyber Crime Center (NC3) has not participated in official JITs, but NC3 has several times participated in joint operations and investigations with a number of other Member States. The national desk at Eurojust has informed that Denmark has participated in a JIT with Germany regarding online fraud committed in Germany and aimed at costumers in Denmark. At the moment, Denmark is also involved in a JIT regarding trafficking in human beings where the crime has taken place also via the use of internet services, and electronic identities and signatures.

The Danish Police cooperates with other LEA in both EU and third countries. There are special rules in the Danish Act on Processing of Personal Data that regulate transferring of personal data to other countries.

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:

end of the questionnaire]