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 *

Federal Ministry of Justice and Consumer Protection

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?

Federal Ministry of the Interior

Optional inclusion of files

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

Please find English translations of German law indicated in the answers at:
http://www.gesetze-im-internet.de/Teilliste_translations.html

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?

Voluntary cooperation

As a rule, the police and the prosecutor's office are both allowed to approach private sector service providers for voluntary cooperation without as part of their general competence to investigate according to Sections 161 (1) and 163 (1) Code of Criminal Procedure. This applies to cooperation with both providers of telecommunications services and providers of information society services

Mandatory "cooperation"

Mandatory cooperation requires a legal basis which explicitly authorizes the prosecutor or police to oblige private sector service providers.

Such authorizations are foreseen in the following sections of the Code of Criminal Procedure:

Search and seizure of objects

In accordance with Sections 94 and 98 of the Code of Criminal Procedure objects on which data are stored (e.g. hard disks or servers) or other physical objects, such as hard copy documents may be secured by seizing the storage media.

As a rule, seizing storage media requires that a court order has been issued. In exigent circumstances, seizure may also be ordered by the public prosecutor's office and the police (first sentence of Section 98(1), Code of Criminal Procedure).

Sections 94 and 98 of the Code of Criminal Procedure are generally applicable to measures concerning both providers of telecommunications services and providers of information society services. However, Sections 94 and 98 of the Code of Criminal Procedure do not apply to measures aiming to obtain traffic data from a provider of telecom services; in such cases, Section 100g of the Code of Criminal Procedure will apply.

Under Section 110 (3) of the Code of Criminal Procedure, the examination of an electronic storage medium at the premises concerned by a search may be extended also to cover physically separate storage media insofar as they are accessible from the storage medium, if there is reason to fear that the data sought would otherwise be lost. This also includes emails which are stored on the provider's server. Examination is permitted if there is reason to fear that data or evidence would otherwise be lost, i.e. if the external storage medium cannot be secured in good time. If data relevant to the proceedings are found, they may be secured pursuant to the second sentence of Section 110(3) of the Code of Criminal Procedure.

Physical documents or storage media - Section 95

Physical documents or stored data can also be obtained by an order to produce the relevant storage media according to Section 95 Code of Criminal Procedure. Section 95 Code of Criminal Procedure applies to both providers of telecommunications services and providers of information society services but also does not apply to measures aiming to obtain traffic data from a provider of telecom services.

Subscriber information

Section 100j regulates the collection of subscriber information in the form of customer data, including a subscriber's name and address and assigned subscriber numbers and identification codes. These can be requested from providers of telecommunication services, provided that this is required for the investigation of the case or determination of the suspect's whereabouts (Section 100j, Code of Criminal Procedure). A court order is not required, unless the request concerns data by means of which access to terminal equipment, or to storage media installed in such terminal equipment or physically separate therefrom. In exigent circumstances the order may also be issued by the public prosecution office or the police.

Traffic data

Traffic data may be obtained from providers of telecommunication services through a production order in accordance with Section 100g Code of Criminal Procedure. Section 100g foresees different requirements for such an order, depending on whether it concerns mandatorily retained data or data retained for business purposes.

If the measure refers to mandatorily retained traffic data , collection is permitted only in the case of particularly serious criminal offences within the meaning of the offences listed in Section 100g (2) of the above Code.

In both cases of traffic data collection, a court order is required as rule. Only in urgent cases of urgency which do not concern mandatorily retained data (Section 100g (2) of the above Code) the order can be issued by a public prosecutor. The police may not issue the order by itself, not even in cases of urgency

Content data

Content data can be collected from telecommunication service providers in real time by means of interception of telecommunications under Sections 100a and 100b of the Code of Criminal Procedure.

This requires that a serious criminal offence listed in Section 100a (2) of the Code is suspected and that interception pursuant to Section 100b has been ordered by a court.

In cases of urgency, interception can be ordered by a public prosecutor. In that case, the measure has to be terminated unless a court confirms it within three working days. The police may not order interception by itself, not even in cases of urgency.

Provided all of these requirements are fulfilled, authorities may apply several techniques, ranging from

- traditional telephone interception to
- techniques typically applied in cybercrime related cases, such as

  - surveillance of data traffic on computers with internet access or internet servers and
  - seizing e-mails from a service provider.

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)?

Yes, see above

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?

There are no overall statistics allowing to answer this question.

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.

In the field of cybercrime the term service provider may include internet service providers, hosting service providers, mail service providers, payment service providers or any other companies which provide services on the internet etc.

As there are too many providers and as each provider is more or less important based on the circumstances of the case, it is not possible to name the top 5 providers.

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:

It is difficult to define the “main seat of the service provider”. This term can relate to corporate structures but could also depend on where the main administrative activities are taking place

or from which office a service provider generally handles the cooperation with law enforcement authorities.

The place, where concrete data is stored by a certain service provider is usually not known by the law enforcement authority, prior to requesting a service provider for its cooperation.

In practice this means, that German authorities have to address the office of the service provider, where the required cooperation can be provided by the service provider. If this office is abroad, the authority has to use the available instruments of international cooperation.

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:

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:

Both the Telecommunication Act (Telekommunikationsgesetz, TKG) and the law applicable to information society services (Telemediengesetz, TMG) determine, to which recipients a provider may disclose personal data. These provisions are exhaustive and do not involve foreign authorities (see e.g. sections 113 par. 3 TKG and 14 par. 2 TMG).

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):

German procedural law differentiates between three groups of data, which are

content data
traffic data
and subscriber or user data.

The term content data comprises all data which can be stored or exchanged via telecom services, e.g. a message which is exchanged via e-mail or any other files, such as pictures, videos or music files, etc.

Traffic data refers to information collected, processed or used during the use of telecommunications services and which provides information on the connection established via these services.

Subscriber or user information relates to the identity of an individual subscriber of services, such as name, address, assigned subscriber numbers and identification codes. The IP-address assigned to an individual internet user is also part of the subscriber or user information.

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

According to German domestic law:

× Subscriber data
× Traffic data
× Content data
× Other data

Given that the relevant requirements set out for each measure at 1.1. are fulfilled.

Requirements of the law applicable to the service provider can vary, depending on which jurisdiction is concerned.

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

Other data relates to measures aimed at data stored on a media device (see answer to question 1.1). These measures are not restricted to a certain type of data, as long as such data is stored on a physical device.

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:

see No.6

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?

Typically the request is done by the investigating law enforcement authority (police or prosecutor's office). If necessary the competent court is involved by issuing a warrant.

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?

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?

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?

Timeframe to obtain data varies depending on the requested information. The general timeframe for all service providers is unknown. In cases of ongoing threats to life or physical conditions it is always requested to provide the information as soon as possible. Usually the requested service providers are answering as soon as possible, e.g. within 30 minutes.

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:

It is not possible to answer this question as every service provider is using their own way of transmission, e.g. web portal, secure channel.

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)?

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

In general, evidence gathered by direct request is admissible. However, depending on the specific circumstances of the case, it might not be admissible, if the right of the accused to a fair trial have been breached. In cross boarder cases, the requirements of international law have to be considered as well.

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:

The Budapest Convention is the most important instrument for cooperation with third countries relating to e- evidence. However, requests can also be based on other multilateral or bilateral treaties on international cooperation, which are not specifically focussed on e-evidence. German Practitioners use administrative guidelines (the so called “Richtlinien für den Verkehr mit dem Ausland in Strafrechtlichen Angelegenheiten” RiVASt), which provide an overview of the bilateral and multilateral agreements, which are applicable in relation to a certain country. The guidelines are available at: http://www.verwaltungsvorschriften-im-internet.de/bsvwvbund_05122012_III19350B13002010.htm
In the absence of international treaties applicable to a requested third country also the Act on International Cooperation in Criminal Matters (Gesetz über die Internationale Rechtshilfe in Strafsachen, IRG), can provide a legal basis for MLA.

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

s. 19a

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 overall statistics on outgoing MLArequests.

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 MLA request is usually initiated by the (Länder- level-) prosecutor´s office responsible for the underlying investigation. Depending on the legal basis applicable in relation to the requested country and the general distribution of tasks between Länder- and Federal governments the MLA request is either sent directly or with the involvement of superior authorities on Länder- or both Länder- and federal levels.

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:

s.10a

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?

There are no overall statistics on incoming MLA requests.

Incoming MLA requests are usually processed by the (Länder- level-) prosecutor´s offices. Depending on the legal basis applicable in relation to the requesting country and the general distribution of tasks between Länder- and Federal governments this can require the prior authorization by superior authorities on Länder- or both Länder- and federal levels.

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?

There are no statistics, which would allow to determine an average timeframe. Bilateral MLA agreements concluded by Germany do not provide for any fixed deadlines.

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)?

s. Nr. 20

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:

MLA requests involving only other EU- MSs are sent and received directly by the competent (Länder- level) prosecutor´s offices. The means of transmission depend on the concrete situation and the available channels. The security of the transmission is of high priority.

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

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

Also within the scenario outlined in Nr. 21 the means of transmission chosen by the transmitting authority depend on the concrete situation and the available channels. Also here the security of the transmission is of high priority.

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:

s. Nr. 26a

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:

s. Nr. 27a

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:

When there are indications, that the data in question is located on the territory of a foreign state, the authority in charge of the measure has to resort to the applicable tools of international cooperation.
Eventually this means, that the access to the data is only possible, when it is at least clear, that the data is stored on the territory of a state party to the Budapest Convention and the conditions of Art. 32 b Budapest Convention are fulfilled.

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:

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:

33. To what extent do your authorities use police-to-police cooperation for obtaining cross-border access to electronic evidence? What is the legal framework for such cooperation and what are current practices (e.g. how often, what data, for which purpose)?

Police-to-police cooperation is usually used to prepare judicial exchange of electronic evidence. Often police-to-police cooperation is also used to fulfil judicial exchange of information. The legal framework is based on various bilateral or multilateral agreements like the Convention Implementing the Schengen Agreement.

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:

Depending on the specific circumstances of the case, evidence gathered abroad might not be admissible if the requirements of international law and / or the right of the accused to a fair trial have been breached.

[end of the questionnaire]