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

Finland.

II. Please indicate which organisation you are representing *

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? *

☐ Yes
☐ No

Yes.

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

The Ministry of the Interior, the Office of the Prosecutor General and the National Bureau of Investigation were involved. Answers are mainly based on the drafts prepared by the National Bureau of Investigation.

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?

Police Act (872/2011)
Chapter 1, Section 1 and Subsection 1:
Police duties
The duty of the police is to secure the rule of law; maintain public order and security; prevent, detect and investigate crimes; and submit cases to prosecutors for consideration of charges. The police work in cooperation with other public authorities and with communities and residents in order to maintain security, and they engage in international cooperation pertaining to their duties.

Chapter 4, Section 3:
Obtaining information from a private organisation or person
At the request of a commanding police officer, the police have the right to obtain any information necessary to prevent or investigate an offence, notwithstanding business, banking or insurance secrecy binding on members, auditors, managing directors, board members and employees of an organisation. The police have the same right to obtain information needed in a police investigation referred to in Chapter 6 if an important public or private interest so requires.

In individual cases, the police have the right to obtain from a telecommunications operator and a corporate or association subscriber on request contact information about a network address that is not listed in a public directory or data identifying a network address or terminal end device if the information is needed to carry out police duties. Similarly, the police have the right to obtain postal address information from organisations engaged in postal services.

For licence administration purposes, the police have the right to obtain information from private organisations and persons as provided in section 2(2–3).

Criminal Investigation Act (805/2011)
Section 1
The authorities in the criminal investigation
(1) The criminal investigation is conducted by the police.
(2) In addition to the police, the border guard, customs and military authorities are criminal investigation authorities as provided in respect of their criminal investigation competence in the

Border Guard Act (578/2005), the Act on the Customs Investigation Office (623/2015), the Military Discipline Act (331/1983) and the Act on the Performance of Police Functions in the Defence Forces (1251/1995). (629/2015)
(3) In addition to the criminal investigation authorities, the prosecutor participates in the criminal investigation.

Coercive Measures Act (806/2011)
Chapter 8, Section 24 and Subsections 1 and 2
Data retention order
(1) If, before the search of data contained in a device, there is reason to assume that data that may be of significance for the clarification of the offence is deleted or is changed, an official with the power of arrest may issue a data retention order. Such an order requires that a person holding or administering data, not however the suspect in an offence, maintains the data unchanged. The order may apply also to data that can be assumed to be transmitted to a device or information system within the month following the issuing of the order. On request a written certificate shall be given of the order, detailing the data that is the object of the order.
(2) What is provided in subsection 1 applies also to data in a message transmitted by an information system that relates to the origin, destination, routing and size of the message as well as to the time, duration, nature and other corresponding factors of the transmission (*transmission information*). (1146/2013)

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?

No statistics available as concerning requests to domestic service providers. Please note that subscriber details (holder of a telephone number) are usually publicly available unless the concerned subscriber has not asked the service provider to keep his/her details secret from the public.

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.

No statistics available. In Finland, the main network operators are TeliaSonera Oyj, Elisa Oyj, and DNA. In addition, there are a number of virtual operators providing access to the Internet.

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

Yes, both in EU Member States and third countries. A Single Point of Contact is, however, applied and all requests are handled by the International Affairs of the National Bureau of Investigation.

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

Nearly 90 % of our requests concern United States, and approximately 10 % EU Members States of which Luxembourg is the most relevant (Skype).

Country wise statistics of requests can be found in the transparency reports of the major service providers. On the site of Google https://www.google.com/transparencyreport/ there are links to a high number of reports of the ISP community.

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

We apply our domestic legal framework.

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

Direct services are voluntary based.

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 State or third countries?
☐ Yes, both from EU Member States and third countries
☐ Yes, but only from other EU Member States
☐ Yes, but only from third countries
☐ No, this is not covered / allowed

The service providers are not authorities and thus their work is not regulated in a similar way as the work of the authorities. They are mainly bound to the contracts, terms of service and their own policy. There is no legislation allowing a service provider responding to a direct request. Telephone subscriber details are usually available for anyone via specific service numbers or via Internet.

In order to evade future problems, the service providers, however, prefer to have foreign requests channelled via Finnish law enforcement authorities. We have no knowledge of any Finnish service provider who is providing direct services to foreign authorities.

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

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

We differentiate the types of data when applying our legal powers. As concerning subscriber details, please note our Police Act, Chapter 4 and Section 3 (see answer # 1).

For the purpose of using content data and traffic data for criminal investigation there are measure-related definitions in Chapter 10, Sections 3(1) and 6(1) of the Coercive Measures Act (806/2011):

"Telecommunications interception refers to the monitoring, recording and other processing of a message sent to or transmitted from a network address or terminal end device through a public communications network referred to in the Telecommunications Services Act or a communications network connected thereto, in order to determine the contents of the message and the identifying data connected to it referred to in section 6. Telecommunications interception may be directed only at a message that originates from or is intended for a suspect in an offence."

"Traffic data monitoring refers to the obtaining of identifying data regarding a message that has been sent from or received by a network address or terminal end device connected to a telecommunications network referred to in section 3, the obtaining of location data regarding the network address or the terminal end device, or the temporary prevention of the use of the network address or terminal end device."

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

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

There are no provisions concerning direct requests in cases where the service provider is located outside our domestic jurisdiction.

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

11. Do you limit direct requests to cases with specific (e.g. exigent) circumstances or to specific (e.g. serious) crimes?
☐ Yes
☐ No

We are following in the requests sent form our country the restrictions of the foreign service providers, and which may vary. For instance, Microsoft requires that the maximum penalty by statute of the offence has to be at least two years imprisonment. In our centralised handling of the requests, we are also looking into the necessity of a request as we do with other international information exchange, too.

11a. If yes, please explain:

Please see answer # 11.

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 International Affairs of the National Bureau of Investigation is the Single Point of Contact for direct requests to foreign service providers from the Finnish police community and Border Guard. A quality system is applied and all requests are approved by a senior police officer before sending them to the concerned service provider. The same quality system applies to our international requests for legal assistance.

A request includes the same elements as in a request for legal assistance, excluding names of the involved parties. Furthermore, the modus operandi of the act is explained very briefly so that the service provider can independently prioritise their processing of the request. As concerning defamation cases, Facebook requires a detailed description of the act to be able to determine that the provision of records is not conflicting with the principle of freedom of speech.

Consequently, a request include what offence is investigated, the case number, the name of the investigating authority, MO in very brief, the penal provisions applied, what details are needed, references of the provisions of the competency of the requesting party, and references of provisions of confidentiality.

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?

As required by all service providers, the request must be on a letter head paper of the requesting agency and signed by a competent official. The ways to send them to the service providers vary. Facebook has a specific portal for the purpose. Google and Microsoft accept request by e-mail. Some service providers do not and want the request provided by fax or mail (these situation are, however, rare).

As mentioned, we apply a national Single Point of Contact system, which is preferred by most of the service providers, too. Thus we can maintain high quality. As the requests are often related to future request for legal assistance and these are handled by the same Single Point of Contact system, too, we have found centralised handling efficient.

14. Do any specific agreements on direct requests exist (or are currently being negotiated) between your authorities and foreign service providers?
☐ Yes
☐ No

There are no specific written agreements made with foreign service providers. We are maintaining contacts with their representatives for consultation when needed.

We have an oral agreement with the most frequently addressed service providers that they accept only request which have been sent to them from our Single Point of Contact unit.

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?

Our current practise has been explained in the previous answers.

In 2015, there were 270 requests made to foreign service providers directly. This was an increase of 70 % compared to the previous year. Most part concerned obtaining of registration (subscriber) details and logging details. A part concerned also request for preservation of data with the view of a future request for legal assistance.

As concerning requests in 2016 per 25 Aug 2016 the foreign service providers have been addressed as follows:

Facebook	34 %
Google	33 %
Microsoft	11 %
Skype	8 %

The rest 14 % includes requests to a number of service providers and no specific is emerging.

Consequently, nearly 90 % of our request concerns United States (and a few to Canada), and approximately 10 % EU Members States of which Luxembourg is the most relevant (Skype).

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?

The response time to a regular request is usually 1-2 weeks and depending of the topical crime domain. Crime against children and violent crime are prioritised by the service providers and the response is often shorter to requests concerning such crime.

The response time to well justified urgent request can be from few hours to 1-2 days depending on the need of the requesting party and work-load of the service provider.

The response time to an Emergency Disclosure Request is very short. It depends on the time of the day and differences of time zones, but also on what type and how much data is requested. Some of the service providers have a 24/7 service for the purpose. If all systems are working properly, the response time is usually less than 30 minutes and max one hour. The current record time for obtaining subscriber details is seven minutes.

Based on our ten years of experience of co-operation with foreign service providers, they are respecting our deadlines promptly. We would like to emphasise that the requesting party can influence in the matter by preparing a clear request which is understandable at a glance.

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

Currently, approximately half of the responses are provided to us either via a secured channel or via a specific Web portal. The other half of the responses are provided by normal email. One major service provider appears to be preparing a Web portal. If and when this will become true, the majority of responses are provided in a secured way.

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

Yes.

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)?

In Finland free consideration of evidence is applied. Chapter 17, Section 1(2) of the Code of Judicial Procedure reads as follows:

“The court, having considered the evidence presented and the other circumstances that have been shown in the proceedings, determines what has been proven and what has not been proven in the case. The court shall consider the probative value of the evidence and the other circumstances thoroughly and objectively on the basis of free consideration of the evidence, unless provided otherwise in law.”

We handle the provided data in the same way as we do with data provided from any domestic service provider. During our ten years of experience of co-operation with foreign service providers, we have no knowledge that the provided information would have been false, or faced any other obstacles.

Furthermore, please note that often the provided data from a foreign service provider is a part of a multiphase procedure to trace and obtain the final evidence to be used. For instance, the subscriber and traffic data (logging details) does not identify the suspect yet, but the provided IP addresses and time stamps can lead to a positive identification when addressing the next request to a domestic service provider.

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?
☐ Budapest Cybercrime Convention
☐ Other multilateral conventions
☐ Bilateral agreements

As the needed electronic evidence is in most cases located in the United States, the Cybercrime Convention is most frequently applied. Concerning Estonia, we have a bilateral agreement which can be applied, too.

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

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

We have bilateral crime prevention agreements with several countries, but the one with Estonia is the most topical in this context.

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)?

United States and Canada.

The number of requests to the United States has been approximately ten per year, but has been rapidly growing and will probably be dozens this year. Canada is addressed with few MLA request per year and are related to the services of KIK Inc.

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?

As mentioned in answer # 1, the criminal investigation is conducted by the police. The Head of the concerned investigation is responsible of the request. The investigation shall always consult the prosecutor of the case in regard the necessity of evidence and the content of the letter rogatory (as the prosecutor in the case is responsible of the evidence to be presented in court. Most often the International Affairs of the National Bureau of Investigation is consulted prior the request in order to find out the specific requirements to be considered and as the International Affairs will conduct a final quality control of the request before it will be signed and translated. Formal MLA requests go through the Central Authority (Ministry of Justice) abroad (e.g. to the US authorities).

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

Content data.

Please note that the subscriber data and traffic data (logging details) provided from the concerned service provider are usually needed in order to better justify the need for the content data and to meet the standards of probable cause in the United States. If the possibilities for obtaining certain data from the service provider directly would not exist, in many cases the procedure would include, in fact, two requests for legal assistance; the first for obtaining subscriber and traffic data, and the second for obtaining content data.

As the foreign service providers accept direct preservation of data request, too, other channels for the purpose is rarely applied.

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

23. Could you explain the situation for incoming Mutual Legal Assistance requests from third countries? How many requests are received per year? Which are the "top" countries that you receive requests from? What kinds of data are usually requested? Which authorities are involved when processing such a request?

Whether an incoming request is sent from outside EU or from an EU Member State, it will land in the International Affairs of the National Bureau of Investigation. No statistics are available in regard to what crime domain the incoming requests are concerning or what measures are requested.

Generally speaking, our neighbouring countries are sending most of the request for legal assistance.

The International Affairs of NBI is checking that the request is generally valid, technically possible to execute and that there are no grounds for refusal. They will also determine to what investigative entity the request will be sent to, and, if needed, consult the available options. Thus possible deadlines, work-load, and available resources can be taken in consideration.

Once the investigative unit has been selected, they will carry out the request and apply, if needed, for court authorisations. Once the requested measures have been conducted, the data will be provided to the International Affairs for forwarding it with a proper cover letter to the requesting country.

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?

As mentioned, the United States is the most frequent country in the matter. The response time is depending on what type of data is requested. As concerning content data, the response time is

usually between 6-12 months, but can be even longer. The record response time is six weeks, but the case was exceptional.

If only subscriber and logging details are needed (from a service provider which does not provide the data directly, such as Yahoo or Twitter), the response time is 1-2 months.

The Finnish investigation and the prosecutor of the case are informed of the response times. Thus they can consider the necessity of their request in relation to other evidence available. In severe cases it can be obvious that the proceedings will continue in a Court of Appeal. In such circumstances the investigation and prosecutor may not wait for the reply to arrive before the proceedings at the first instance.

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)?

In the United States, the matter will not be presented before a court unless the provided information in the request is considered to be sufficient enough. Therefore we have not faced a situation where the final decision maker would have refused.

The challenge is to provide probable cause that an account or profile belongs to the suspect, and probable cause that the account or profile has been used in the criminal act under investigation. Sometimes the situation can be conflicting; the case is highly prioritised, but the needed evidence for obtaining additional evidence is scarce. Then we may consult US Department of Justice prior to a request and may even provide a draft for comments.

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

The matter is depending of the amount of documents and the urgency of the matter.

We miss a joint system for encrypted emails for fast electronic messaging between judicial authorities, those indicated in the EJN Atlas. In urgent situation we may send the request to the NCB of Interpol of the concerned country.

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

27. What are the means of transmission of Mutual Legal Assistance requests to third countries (how you send it)?
☐ Regular mail (letter)
☐ Fax

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

Request to countries outside EU are forwarded via our central authority which is the Unit for International Judicial Administration, Ministry of Justice.

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

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

The matter is depending on the form and amount of data.

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

If no other option is available and the matter is urgent or sensitive, we may send our reply with a commercial courier (UPS or similar).

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

The matter is depending on the form and amount of data. The formal reply is always channelled via our central authority, but sometimes we need to agree of the provision of the material in itself separately.

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

As we have regular working meetings with a representative of a FBI Legal Attaché Office, we often receive and provide the material personally.

If no other option is available and the matter is urgent or sensitive, we may send our reply with a commercial courier (UPS or similar).

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:

Finland has no legislation concerning this issue.

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:

Finland has no legislation concerning this issue.

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:

Please see the previous answers.

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

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

☐ Yes
☐ No
☐ It depends on circumstances

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

[end of the questionnaire]