www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Strasbourg, 15 February 2012 T-CY (2012)04

Cybercrime Convention Committee (T-CY)

Assessing implementation of the Budapest Convention on Cybercrime

Questionnaire on preservation measures (Articles 16, 17, 29, 30)

Background:

The purpose of the questionnaire is to allow the T-CY Plenary to assess the implementation of Articles 16, 17, 29, 30 of the Budapest Convention on Cybercrime by State Parties.

The Cybercrime Convention Committee (T-CY), in its 6th Plenary Session (23-24 November 2011) decided:

– "To review at the first Plenary in 2012 the implementation by the Parties of articles 16, 17, 29 and 30 (Action 3.1 of the Plan), and to encourage Parties to cooperate with the Bureau and the Secretariat in this respect."

The Bureau of the T-CY prepared the present questionnaire in its meeting on 30-31 January 2012. It requested the Secretariat to send it to T-CY representatives with copy to Permanent Representations by 15 February 2012.

Implementation:

T-CY representatives are invited to prepare/compile consolidated replies to this questionnaire from their respective country.

Replies should be submitted no later than **15 April 2012** in electronic form and in English or French to:

Alexander Seger, Secretary of the Cybercrime Convention Committee, DG 1, Council of Europe
Email: alexander.seger@coe.int

T-CY members will then receive a draft analytical report by 15 May 2012 for comments. The report will subsequently be discussed at the 7th T-CY Plenary on 4-5 June 2012. Parties to the Budapest Convention should be prepared to present their preservation system during that meeting.

The final report, which will be completed after the 7th Plenary, will assess the implementation of these articles of the Budapest Convention, make suggestions to further enhance their effective implementation and document good practices.

1 Article 16 – Expedited preservation of stored computer data (domestic level)

1.1 Legislation/regulations

Q 1.1.1 What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

Q 1.1.2 Do they cover all types of data (traffic, content) stipulated by article 16?

Q 1.1.3 Do they apply to electronic evidence in relation to any criminal offence or are there limitations? Please explain.

Q 1.1.4 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

Q 1.1.5 Is preservation visible to the suspects or account holder or can you prevent disclosure of the preservation request?

1.2 Procedures

Q 1.2.1 Please describe the end-to-end procedure for the handling of a request.

Q 1.2.2 What templates/forms are used? Please attach if any.

1.3 Practical experience

Q 1.3.1 How relevant to investigations in your country is expedited preservation? How relevant is expedited preservation compared to other measures (e.g. production order, search and seizure)? Without provisions on preservation, would this create problems for your investigations?

Q 1.3.2 How frequently do you use these provisions? Please provide estimated numbers on preservation requests if readily available.

Q 1.3.3 Is preservation in your country a measure specifically foreseen in the procedural law, or do you need to order preservation through search, production order or other powers?

Q 1.3.4 Do you ever serve preservation requests to physical or legal persons other than service providers?

Q 1.3.5 In general terms, how do you rate service provider cooperation in the execution of preservation requests?

Q 1.3.6 Please describe a typical case or scenario.

Q 1.3.7 In conclusion: What are the main strengths and what are the main problems of your preservation system?

2 Article 17 – Expedited preservation and partial disclosure of traffic data (domestic level)

2.1 Legislation/regulations

Q 2.1.1 What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

Q 2.1.2 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

2.2 Procedures

Q 2.2.1 Please describe the end-to-end procedure for the handling of a request.

2.3 Practical experience

Q 2.3.1 How relevant to investigations in your country is partial disclosure?

Q 2.3.2 How frequently do you use these provisions?

Q 2.3.3 In general, what is the response time by service providers?

3 Article 29 – Expedited preservation of stored computer data (international level)

Please refer to your replies on articles 16 or 17 if applicable.

3.1 Legislation/regulations

Q 3.1.1 What legal provisions/regulations do you apply for executing an international request for preservation? Please list and attach text.

Q 3.1.2 Who has the competence for receiving and executing the international preservation request? What is the role of the contact point?

Q 3.1.3 What rules apply for the transfer of the data preserved to foreign authorities?

3.2 Procedures

Q 3.2.1 Please describe the end-to-end procedure for the handling of the request.

Q 3.2.2 What templates/forms are used for international requests? Please attach if any.

Q 3.2.3 Other than the information listed in Article 29.2, what information do you need in order to execute a request?

3.3 Practical experience

Q 3.3.1 How frequently do you send and receive international preservation requests? Please provide estimated numbers if readily available.

Q 3.3.2 In general, as a requested country, how quickly do you issue a preservation request?

Q 3.3.3 In general, as a requesting country, how quickly are you notified that your request has been issued in the foreign country?

Q 3.3.4 Please describe a typical case or scenario.

Q 3.3.5 Without provisions on preservation, would this create problems for international cooperation?

Q 3.3.6 How often are international preservation requests that you receive not followed by mutual legal assistance requests?

Q 3.3.7 How often do you send international preservation requests and not follow them with mutual legal assistance requests or notifications?

Q 3.3.8 In conclusion: What are the main strengths and what are the main problems of preservation within the framework of international cooperation?

4 Article 30 – Expedited disclosure of preserved traffic data (international level)

Please refer to your replies on articles 16 or 17 if applicable.

4.1 Legislation/regulations

Q 4.1.1 What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

Q 4.1.2 What are the conditions, limitations or impediments to disclosing a sufficient amount of traffic data?

4.2 Procedures

Q 4.2.1 Please describe the end-to-end procedure for the handling of a request.

4.3 Practical experience

Q 4.3.1 How frequently do you use this provision?

Q 4.3.2 Please describe a typical case or scenario.

Q 4.3.3 Without provisions on partial disclosure, would this create problems for international cooperation?

Appendix: Extracts of the Budapest Convention on Cybercrime

Title 2 – Expedited preservation of stored computer data

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;

b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

c the stored computer data to be preserved and its relationship to the offence;

d any available information identifying the custodian of the stored computer data or the location of the computer system;

e the necessity of the preservation; and

f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.