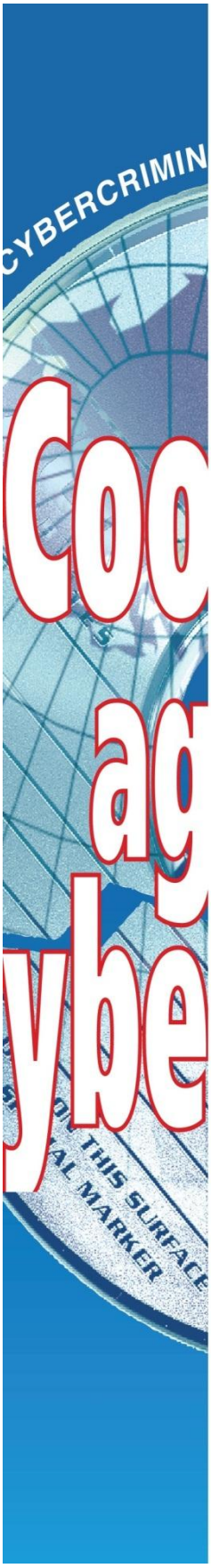

Cybercrime Convention Committee (T-CY)

Assessment report

Implementation of the preservation provisions of the Budapest Convention on Cybercrime

Adopted by the T-CY at its 8th Plenary (5-6 December 2012)

T-CY (2012)10 REV

Strasbourg, 25 January 2013 (provisional)

www.coe.int/TCY

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Contents

Contact

Alexander Seger
Secretary of the Cybercrime Convention Committee (T-CY)
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int

1 Introduction

The Cybercrime Convention Committee (T-CY) decided, at its 6th Plenary Session (23-24 November 2011), to "review the effective implementation of the Budapest Convention by the Parties".[1]

Specifically, the Parties agreed to review in 2012 the expedited preservation provisions of:

- Article 16 – Expedited preservation of stored computer data (domestic level)
- Article 17 – Expedited preservation and partial disclosure of traffic data (domestic level)
- Article 29 – Expedited preservation of stored computer data (international level)
- Article 30 – Expedited disclosure of preserved traffic data (international level).

The purpose of this report is to enhance the practical application of the Budapest Convention on Cybercrime by assessing its implementation by the Parties, by identifying good practices, by helping address problems encountered and by sharing experience between current and potential future Parties to this treaty.

With regard to the four articles analysed, the report should

- provide a better understanding of the difference between the concept of expedited preservation (articles 16, 17, 29 and 30) and the concept of data retention (not foreseen in the Budapest Convention but implemented in many States, for example, under the European Union Data Retention Directive)
- encourage the use in practice of the preservation provisions in domestic and international investigations
- promote a stronger role of the 24/7 points of contact in securing electronic evidence in international cooperation.

A questionnaire, prepared by the T-CY Bureau in January 2012, was sent to T-CY Representatives with copy to Permanent Representations on 15 February 2012.[2]

The T-CY, at its 7th Plenary Session on 4-5 June 2012 discussed a first version of the present assessment report and adopted preliminary conclusions.[3] It was decided to complete the assessment of the four provisions at the 8th Plenary in December 2012.

The 8th Plenary of the T-CY adopted the assessment report in principle subject to additional information to be provided by some Parties.

The final version report was adopted by the T-CY following a written procedure on 25 January 2013.

---

[1] Objective 3 of the Workplan for the Period January 2012 to December 2013.
http://www.coe.int/t/dghl/standardsetting/t-cy/T-CY_2011_10E_PlenAbrMeetRep_V4%20_28Nov2011.pdf

[2] In the light of a study being undertaken in parallel by the European Commission (DG Home) on the implementation of data preservation and data retention provisions, and in view of avoiding redundancies, it was agreed to consolidate the questionnaires of the T-CY and the European Commission, and that Parties would reply to both at the same time. The European Commission (DG Home) had contracted the consulting firm Centre for Strategy and Evaluation Services (CSES) for the preparation of its study.

[3] Appendix 2 of the abridged meeting report
http://www.coe.int/t/dghl/standardsetting/t-cy/TCY2012/TCY_2012_14E_PlenAbrMeetRep_V7_21june2012.pdf

Replies received:

Party	**Replies received**[4]
1. Albania	7 July 2012
2. Armenia	18 April 2012
3. Azerbaijan	6 April 2012
4. Bosnia and Herzegovina	18 April 2012
5. Bulgaria	7 May 2012
6. Croatia	13 April 2012
7. Cyprus	11 September 2012
8. Denmark	[no replies received]
9. Estonia	14 May 2012
10. Finland	13 April 2012
11. France	13 April 2012
12. Georgia[5]	13 July 2012
13. Germany	13 April 2012
14. Hungary	18 April 2012
15. Iceland	[no replies received]
16. Italy	24 September 2012
17. Latvia	12 April 2012
18. Lithuania	20 April 2012
19. Republic of Moldova	9 April 2012
20. Montenegro	14 May 2012
21. Netherlands	16 April 2012
22. Norway	24 April 2012
23. Portugal	1 May 2012
24. Romania	18 April 2012
25. Serbia	26 April 2012
26. Slovakia	5 November 2012
27. Slovenia	13 April 2012
28. Spain	18 May 2012
29. Switzerland	18 September 2012
30. "The former Yugoslav Republic of Macedonia"	3 May 2012
31. Ukraine	16 April 2012
32. United Kingdom	25 May 2012
33. United States of America	14 April 2012
Total	**31**

[4] Some Parties subsequently provided additional information.

[5] Australia (November 2012) acceded to, and Austria (June 2012), Belgium (August 2012), Georgia (June 2012), Japan (July 2012), Malta (April 2012) ratified the Budapest Convention after the assessment exercise had been launched. Georgia nevertheless agreed to provide replies to the questionnaire.

2 Implementation of Articles 16 and 29 on expedited preservation

2.1 About Article 16 – Expedited preservation (domestic level)

Article 16 is a provisional measure that allows the authorities to order the immediate preservation of data already stored on a computer system. This may include traffic but also content data, and it may include data held by a service provider, but also by any other physical or legal person. Expedited preservation refers to specified computer data that may be required in a specific criminal investigation. While the integrity of volatile data needed for a criminal investigation may also be secured through search and seizure (article 19) or a production order (article 18) such measures often require more time, justification and authorisation than the provisional measure of expedited preservation and maybe be more visible to the suspect. Implementation of Article 16 is to allow for the time necessary to obtain the authorisation for the measures under articles 18 and 19. This is particularly important in the context of international cooperation where the provisional measures of articles 29 and 30 allow for the time needed for mutual assistance, in particular requests for stored computer data in another country (article 31).

Article 16 is not a data retention obligation. It is narrower in that it refers to specified computer data needed in a specific investigation and still stored on a computer system (which means that often at the time of the request the data is not available anymore). And it is broader in that it not only covers subscriber and traffic data (as foreseen in data retention regulations) but also content data, and in that it not only covers service providers but any physical or legal person that may hold computer data needed in an investigation.

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.

2.2 Implementation of Article 16: overview

When assessing implementation of Article 16 by the Parties, the T-CY uses the following criteria:

- Do law enforcement authorities have the lawful power:
  - to order any legal or physical person holding data
  - to preserve or similarly obtain electronic evidence in an expedited manner
  - in relation to any crime?

- Has this power been applied in practice?

2.2.1 Regulations providing powers[6]

About half of the Parties have adopted specific regulations allowing for the expedited preservation of stored computer data while others rely on other powers to preserve evidence. Most Parties have also established data retention obligations.

Specific legal provisions on expedited preservations have been put in place to transpose Article 16 into domestic law:

- Albania: Article 299/a Criminal Procedure Code (CPC)
- Bulgaria: Article 159 CPC
- Finland: Coercive Measures Act, Chapter 4, Sections 4b and c
- France: Art 60-2 CPC
- Hungary: Section 158/A CPC
- Italy: Several provisions through Law 48 of 2008
- Latvia: Section 191 CPC
- Moldova: Article 7 of Law on preventing and combating cybercrime (No 20-XVI of 3 February 2009)
- Netherlands: Article 126ni of Dutch Code of Criminal Procedure
- Norway: Section 215a Criminal Procedure Act
- Portugal: Article 12 of the Law on Cybercrime (Law nº 109/2009)
- Romania: Article 54 of Law 161/2003
- Slovakia: Article 90 of the Code of Criminal Procedure
- USA: U.S. Federal Criminal Code, Title 18, Section 2703(f)

Other Parties report the use of search and seizure, production orders or similar powers to preserve electronic evidence. These approaches are valid in the meaning of the Budapest Convention, if such powers permit to secure electronic evidence in relation to any crime and any legal or physical person holding data in an expedited manner.[7] The Budapest Convention does not necessarily require that

[6] See appendix for extracts of domestic legislation.

[7] Discussions during the T-CY Plenary in December 2012 showed that Parties have different views as to whether a Party meets the requirements of the Budapest Convention if, in the absence of specific preservation orders, powers such as search, seizure or production orders are used. Most Parties would agree that such an approach is valid if such powers indeed permit to secure electronic evidence in relation to any crime and any legal or physical person holding data in an expedited manner.
Some Parties, on the other hand, are of the opinion that (a) the Budapest Convention allows for search, seizure and similar as alternatives to preservation, and that (b) such powers may be limited in line with Article 15 (conditions and safeguards). The assessments in the present report are based on the first approach:

Parties establish a specific provision in their criminal procedure law, but general procedural powers can be used. As stated in the Explanatory Report:

> 160. The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor). In some States, preservation orders do not exist in their procedural law, and data can only be preserved and obtained through search and seizure or production order. Flexibility is intended by the use of the phrase 'or otherwise obtain' to permit these States to implement this article by the use of these means. However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases.

Nevertheless, as suggested in the last sentence of paragraph 160 Explanatory Report, even if other powers can be applied, it may still be more effective to establish specific preservation powers.

In some countries, service providers or other legal or physical persons seem to be prepared to voluntarily preserve data pending a formal production order. In some cases, additional arrangements have been made with service providers:

- In Azerbaijan, under an administrative measure, service providers have appointed dedicated "curators" who can be asked by the Ministry of National Security to "informally and expeditiously order the preservation of data"
- In Georgia a Memorandum of Understanding between law enforcement and Internet service providers was signed in May 2010
- In Lithuania, under an agreement, the largest national providers give access to law enforcement to traffic and subscriber information
- In the Republic of Moldova, the General Prosecutor's Office and the National Bank of Moldova signed an agreement on electronic money and electronic commerce.
- In Norway, the largest domestic ISP has made arrangements for a 24/7 police response centre and large transnational providers accept requests directly under certain conditions. Specific agreements have also been concluded with a number of ISPs regarding the filtering of child abuse images
- In Romania good practices have been developed regarding law enforcement/ISP cooperation.

2.2.2 Any type of data

Most Parties replied that all data in the meaning of Article 16 would be covered under their regulations (subscriber information/traffic and content data). Exceptions seem to include Armenia and Ukraine with data limited to traffic data. In Germany, separate provisions are used for the search and seizure of traffic and of other data.

In the absence of specific preservation provisions it is acceptable that Parties make use of alternative provisions to "similarly obtain" the securing of specified data, including traffic data, if this is possible in an expedited manner and with respect to all types of data. If the use of such alternative provisions is restricted, a Party is considered "not in line" or "partially in line", depending of the extent of such restrictions. Most Parties are of the opinion that specific provisions for the provisional measure of data preservation would allow respecting the conditions and safeguards of Article 15 before obtaining data through search, seizure or disclosure.

Almost all Parties (with the exception of Armenia, Germany, Norway[8] and the USA) also rely on data retention obligations and make extensive use of retained data. However, such obligations are limited to traffic data while Article 16 also covers content data.

Parties only referring to data retention obligations would therefore not be fully implementing Article 16.

2.2.3 Any type of crime

Article 16 is designed as a measure to preserve data in relation to any crime not only with respect to offences against or by means of computer systems (see Article 14 (2) on the scope of procedural provisions), and not only in relation to serious crime.

Most Parties are able to apply preservation orders with respect to any crime. In some countries additional tools are available in cases of serious or organised crime.

As indicated, most Parties have established data retention obligation as required under the EU Data Retention Directive of 2006. This Directive contains a purpose limitation (access to traffic data to investigate serious crime) and many Parties have followed this approach. Such a purpose limitation is not foreseen in Article 16. Therefore again, Parties only referring to data retention obligations would not be fully implementing Article 16.

Moreover, it has also been suggested that the purpose limitation for law enforcement access to retain traffic data could lead to a situation where there are lower requirements for law enforcement access to content data than for traffic data.

Most Parties comply with Article 16 (3) and oblige the person or entity requested to preserve data to keep the undertaking of such a measure confidential. In Norway, the individual whose data has been preserved will need to be informed at the latest when law enforcement has access to the data unless a court has decided otherwise.

2.2.4 Any legal or physical person holding data

Most electronic evidence sought for law enforcement purposes is likely to be held by service providers, and most Parties have established legal powers, sometimes complemented by cooperation arrangements, to order service providers to preserve data or to access data held by service providers. Data retention obligations are also limited to service providers.

However, Article 16 covers also other legal as well as physical persons.

Some Parties have not fully implemented this requirement and preservation systems are limited to service providers only.

2.2.5 Procedures for expedited preservation

The expedited preservation of data at the level of a service provider, operator or other custodian of data is a provisional measure that should be ordered without delay and allow for the time needed to seize or order the production of data with the necessary authorization by a judicial authority.

[8] In Norway, a data retention law was adopted by Parliament in 2011 but entry into force has been postponed.

In countries where specific legal provisions are in place, this requirement of expedited action appears to be met and a prosecutor (most countries) or investigator (some countries) and in the USA any government official can order specified computer data in relation to any crime to be preserved.

In most countries where other measures are used, the procedure usually involves a court order for search and seizure or production order. Such a judicial decision may be obtained within 24 hours but could also take several weeks. In exigent circumstances or other conditions, a prosecutor or even police officer may take such measures.

As noted earlier, "expedited preservation" is a provisional measure to take immediate action to secure volatile electronic evidence and to give time for formal procedures required for the actual disclosure of data.

This means that – in line with Article 16 – conditions for a preservation order or, alternatively, to similarly obtain the securing of electronic evidence through search, seizure or production orders should not be too restrictive or complex but should be possible in an expedited manner.

Specific powers to order preservation as a preliminary measure are thus preferred. Sufficient time to obtain authorisation search, seizure or production orders will allow for judicial oversight or other safeguards.

2.2.6 Applied in practice

Most Parties consider the expedited preservation provision an important tool. However – with the exception of the USA where many thousand preservation orders are issued every year – the actual application of Article 16 in Europe appears to be more limited, in particular with respect to domestic investigations.

While it is frequently used in some countries (such as Bulgaria and Moldova), most Parties report that their criminal justice authorities prefer to apply search and seizure provisions or production orders directly, and in most cases were not in need of the provisional preservation of data. Information provided also suggests that this was different in cases of international requests where domestic judicial orders for search, seizure or production of data were more difficult to obtain and provisional measures were needed to preserve evidence.

2.2.7 Practices

2.2.7.1 Norway: relevance of preservation

Expedited preservation is relevant primarily with regard to international requests. A lack of provisions on preservation would create significant problems in cases where electronic evidence is available, but outside Norway. Legal requests take time, and data would most likely be deleted or altered before the request could be processed. One example: in a recent murder case in Norway, it took one year for the Norwegian police to get access to content data from Facebook. The evidence arrived in Norway during the trial, and proved to be important to the result of the case: both defendants were found guilty, and the appeals court upheld the verdict.

In Norway, the largest domestic ISP has made arrangements for a 24/7 police response centre and large transnational providers accept requests directly under certain conditions.

The largest part of these cases is not preservation orders addressed to the police of other countries, but requests form police or prosecutors in Norway to a limited number of large, multinational services

(Facebook, Google, Microsoft etc.) to freeze data. Some of these companies have 24/7 response teams for law enforcement requests.

The fact that these companies accept requests to freeze data from police outside their own jurisdiction is most likely based on the fact that these companies in any case would be covered by international provisions for expedited preservation (if they are Party to the Budapest Convention). This practice reduces the workload for the police, but does not reduce the rights and legal protections for their customers. To obtain content data, it is always necessary to send a legal request to the country where the company in questions is located.

There is reason to believe that a lack of provisions on preservation would lead to the indirect result that companies like Facebook and Google would no longer accept or process "freeze requests" from police in other countries.

Sometimes preservation orders are also served to Norwegian third parties. Requests to the court for a production order would take a longer time to process than a production order issued by the prosecution authority.
In cases regarding data of sensitive character, such as data that may be covered by a duty of confidentiality, it may be preferable to get a production order issued by the court, to make sure that due process is followed. Without a preservation order, it is possible that the prosecutors would issue more production orders, and the courts would get fewer requests.

It is not necessary to use a preservation order to get basic subscriber information from telecom companies, ISPs and several Internet services (Facebook, Microsoft etc.).

2.2.7.2 USA: relevance, strengths and issues

Preservation is a crucial and often-used tool for US investigations. It gives investigators and prosecutors time to obtain the necessary legal process to compel a service provider to disclose data. Thus, preservation is generally a first step towards obtaining data held by service providers. A preservation request is not a request for disclosure of data; the request does no more than require the provider to hold on to stored data. Data preserved by a service provider is not available to investigators or prosecutors until appropriate legal process (a subpoena, court order, or warrant) is issued to the service provider.

The US does not have a data retention law, so—absent a preservation request for a particular account—providers are free to keep or delete account holder data based on the providers' business practices. Without data preservation, investigators would lose access to a significant amount of data.

Main strengths:

- any law enforcement official may issue a preservation request
- the preservation request process is simple and quick
- preservation gives investigators up to 180 days to take necessary investigative steps to obtain legal process to compel disclosure of the data
- disclosure of data must be authorized by a separate legal process

Main problems:

- investigators will usually not obtain any data about the account, including whether the account exists, because service providers are prohibited by law from disclosing such data without further legal process

- although most major providers keep preservation requests confidential, service providers are permitted to disclose a preservation request to the account holder. This may prematurely disclose and damage an investigation.

2.3 About Article 29 - Expedited preservation of stored computer data (international level)

Article 16 has its equivalent in Article 29 for international preservation requests. While at the domestic level production orders or search and seizure provisions may be used to secure volatile data, at the international level preservation requests may often be the only means to secure electronic evidence related to any crime in another country pending a mutual legal assistance request.

Under Article 35 Parties are to establish 24/7 points of contact to facilitate the sending and execution of international preservation requests.

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.

2.4 Implementation of Article 29: overview

2.4.1 Regulations providing powers

Some Parties have adopted specific regulations on international preservation requests, such as:

- Portugal: Articles 22 and 23 of the Law on Cybercrime (Law nº 109/2009)
- Republic of Moldova: Article 10 of the Law on Preventing and Combating cybercrime (No 20-XVI of 3 February 2009)
- Romania: Articles 63 and 64 of Law 171/2003

Parties without specific provisions for international requests but with specific powers for domestic preservation procedures report that they can apply these, for example, under laws on international cooperation in criminal matters or by referring to Article 29 Budapest Convention to which they are Parties.

As indicated, a number of Parties use search, seizure, production orders or other general procedural powers to secure electronic evidence in the absence of specific preservation provisions. In these States, follow up to international preservation requests appears to be more complicated. It seems that often a formal MLA request is required followed by a court order to permit the use of such powers and secure data.

This may explain the very low number of international preservation requests in Parties without specific preservation powers.

2.4.2 Role of 24/7 points of contact

In order to facilitate the application of Articles 29 and 30 in practice, Article 35 Budapest Convention requires Parties to establish 24/7 contact points.

All Parties have established such contact points. Some of these seem to be active in sending, receiving and following up to international preservation requests. Some others are less active even though they have the necessary powers. A number of contact points, finally are not able to send, receive or follow up to international requests since the domestic legal basis for preservation is weak or involves a formal mutual legal assistance procedure.

Party	24/7 point of contact	Authority and role regarding sending and executing preservation requests
1. Albania	Sector against Computer Crime, Ministry of Interior	Authorised to send/receive requests for preservation. Follow up by Office of Prosecutor General
2. Armenia	Division for High Tech Crime, Main Department Fighting Against Organised Crime in the Police	24/7 CP cannot issue preservation orders in the absence of domestic powers
3. Azerbaijan	Department of Combating Crimes in Communications and IT Sphere, Ministry of National Security	Authorised to send/receive and follow up to requests for preservation
4. Bosnia and Herzegovina	International Police Cooperation Sector, Interpol, Sarajevo	Authorised to send/receive and follow up to requests for preservation
5. Bulgaria	Cybercrime Section, Chief Directorate for Combating Organised Crime, Ministry of the Interior	Authorised to send/receive and follow up to requests for preservation.
6. Croatia	Department for Economic Crime and Corruption, General Police Directorate	Authorised to send/receive and follow up to requests for preservation
7. Cyprus	Office for Combating Cybercrime and Forensic Lab, Cyprus Police Headquarters	Authorised to receive requests to forward them to Ministry of Justice for verification and further action
8. Denmark	Danish National Police	
9. Estonia	Bureau of Criminal Intelligence	Authorised to send/receive and follow up to requests for preservation
10. Finland	National Bureau of Investigation Alternative CP: Ministry of Justice	Authorised to send/receive and follow up to requests for preservation
11. France	Office Central de Lutte contre la Criminalité liée aux Technologies de L'Information et de la Communication (OCLCTIC) Judicial Police, Ministry of Interior	Authorised to send/receive and follow up to requests for preservation
12. Georgia	Criminal Police Department Ministry of Internal Affairs of Georgia	The powers of the newly established contact point are yet to be tested
13. Germany	National High Tech Crime Unit, Federal Criminal Police Office (BKA)	Authorised to send/receive and follow up to requests for preservation
14. Hungary	International Law Enforcement Cooperation Centre of the Police Alternative CP: National Bureau of Investigation High-tech Crime Unit	Authorised to send/receive and follow up to requests for preservation
15. Iceland	National Commissioner of the Icelandic Police	
16. Italy	Servizio Polizia Postale e delle Comunicazioni Alternative CP: Office of District Attorney of Rome – Cybercrime section	Authorised to send/receive and follow up to requests for preservation
17. Latvia	Operational Coordination and Information Provision Unit, State Police of Latvia	Authorised to send/receive and follow up to requests for preservation

18. Lithuania	Cybercrime Unit, Lithuanian Criminal Police Bureau	Authorised to send/receive and follow up to requests for preservation (Order of Police Commissioner General No. 5-V-1102, 12 December, 2011) However, no requests sent/received to date
19. Republic of Moldova	Section for Combating IT crimes, Chief Prosecutor's Office And: High-tech Crime Unit	Both are authorised to send/receive and follow up to requests for preservation
20. Montenegro	Police Directorate of Montenegro	Authorised to send/receive and follow up to requests for preservation (via Prosecutor and Court)
21. Netherlands	National High Tech Crime Unit (NHTCU), National Police National Prosecutor Office	Both are authorised to send/receive and follow up to requests for preservation
22. Norway	High-Tech Crime Division, KRIPOS National Criminal Investigation Service (NCIS Norway)	Both are authorised to send/receive and follow up to requests for preservation (as well as MLA requests)
23. Portugal	Coordinator of Criminal Investigation in Portugal, Judicial Police	Authorised to send/receive and follow up to requests for preservation.
24. Romania	Service for Cybercrime, Directorate for the Investigation of Organised Crime and Terrorism Offences, Prosecutor's Office attached to the High Court of Cassation and Justice Alternative CP: Cybercrime Unit, General Directorate for Countering Organized Crime and Anti-drugs Bucharest, Romania (National Romanian Police)	Authorised to send/receive and follow up to requests for preservation. The power of the Prosecutor's Office as 24/7 CP is defined in the Law on Cybercrime
25. Serbia	Ministry of Interior Service for Combating Organized Crime - Special Department for High-Tech Crime. Alternative CP: Special Public Prosecutors Office for High-Tech Crime	Special Public Prosecutors Office for High-Tech Crime. MoI Service for Combating Organized Crime - Special Department for High-Tech Crime. Can issue an order to ISP to preserve data within CPC framework of gathering of data request.
26. Slovakia	National Central Bureau of Interpol, International Police Cooperation Office	Authorised to send/receive and follow up to requests for preservation
27. Slovenia	Sector for international police cooperation, Criminal Police Directorate Alternative CP: Cyber Investigation Unit, Criminal Police Directorate	Authorised to send/receive and follow up to requests for preservation
28. Spain	Brigada de Investigación Tecnológica, Comisaria General de Policia Judicial, UDEF Central And: Guardia Civil (GC),Grupo de Delitos Telematicos (GDT) (Computer Crime Unit)	Authorised to send/receive and follow up to requests for preservation

29. Switzerland	Operations Center fedpol	Authorised to send/receive and follow up to requests for preservation
30. "The former Yugoslav Republic of Macedonia"	Basic Public Prosecutors Office in Skopje	Authorised to send/receive and follow up to requests for preservation
31. Ukraine	Cybercrime Subdivision, Division for Combating Cybercrime and Human Trafficking, Criminal Police Department	Authorised to send/receive and follow up to requests for preservation (to be reviewed under the new Criminal Procedure Code of November 2012)
32. United Kingdom	SOCA Cyber	Authorised to send/receive and follow up to requests for preservation
33. United States of America	Computer Crime and Intellectual Property Section (CCIPS), U.S. Department of Justice	Authorised to send/receive and follow up to requests for preservation

2.4.3 Procedures and experience

Typically, an international preservation request is received by the 24/7 contact point who orders a service provider or other legal or physical person to preserve data. Once a formal request for MLA has been received – usually by the Ministry of Justice – and a court order has been issued, the service provider discloses the data to the domestic authorities who then transmit them to the requesting Party.

This procedure – with adjustments to specific domestic conditions – is followed by a number of Parties, in particular where preservation powers are specifically defined by law.

Example: Romania

- An international expedited preservation request sent to the Romanian 24/7 Contact point (via email) is describing a case of intrusion followed by alteration of data. The case is investigated by a local police office in country X. The Romanian authorities are asked to preserve subscriber information and traffic data related to several IP addresses (time and date indicated). According to the letter IP address belong to a provider located in Bucharest.
- After registration in the unit's register, the prosecutor will verify the IP addresses and the provider and then will issue the ordinance for preservation.
- If the information provided by the requesting country is not accurate or the provider no longer exists (even if the company is still mentioned on RIPE etc.), the prosecutor will inform the other party to rectify the request.
- The requesting country is also informed that for getting the information that was preserved a letter rogatory is needed.
- A territorial office in Romania is asking the 24/7 Contact point to forward its expedited preservation request to country X. The local request is describing the facts, specific crime, and is asking for preservation of subscriber information related to an email address (service based in country X) and the login information for a specified period of time. It is also requested the preservation of the email box content.
- The request will be registered in the unit's register and with a cover letter will be sent via email by the Romanian 24/7 Contact Point to the foreign 24/7 Contact Point.

While the USA sends and receives hundreds of preservation requests per year, a few others also make frequent use of this possibility (such as France, Moldova or Romania). It should be noted that reliable statistics on the use of preservation orders are not available as in some countries different services are empowered to send/receive and follow up to preservation requests, often preservation requests may be labelled differently or be part of a broader procedure.

Overall, however, the T-Cy is of the opinion that the option of international preservation requests is underused. Reasons seem to be:

- Unclear legal basis and complex procedures in some countries
- Unclear role of 24/7 contact points
- Limited knowledge and routines in the use of procedure and other channels are used.

2.5 Implementation of Article 16 and 29 (expedited preservation at domestic and international level) – Assessment

Party	Legal provisions and practical experience	Assessment
1. Albania	Regarding domestic procedures (Article 16 Budapest Convention): Albania adopted the specific provision of Art 299/a CPC for expedited preservation. Article 299/a covers any type of data and data in relation to any offence. A preservation order is issued by a prosecutor. It can be addressed to any legal or physical person holding data, not only to service providers. In addition, Article 101 of the Law 9918 on Electronic Communication provides for data retention. Practical experience and use of Article 299/a is limited so far. One problem is the inadequate technical capability of some of the service providers to preserve data. Regarding international procedures (Article 29 Budapest Convention): The specific legal provisions of Article 299/a CPC for preservation at the domestic level in combination with Article 505 CPC, Law 10193 of 2009 on "judicial relations with foreign authorities in criminal matters" and other international treaties can be applied. A 24/7 point of contact has been established at the Sector against Computer Crime, Ministry of Interior. A formal MLA request is required for the collection and transmission of preserved data. In the second half of 2012, Albania began to make practical use of these provisions.	Article 16 Budapest Convention: Albania is in line with Article 16 Budapest Convention. It may be useful to organise additional training for law enforcement and service providers in the practical application of Article 299/a. Article 29 Budapest Convention: Albania is in line with Article 29, and the system is now being used in practice. The legal and institutional framework is in place, and the authorities may promote further application in practice.
2. Armenia	Regarding domestic procedures (Article 16 Budapest Convention): No specific legal provisions are available that meet the requirements of Article 16 Budapest Convention. Electronic evidence is considered material evidence and search and seizure provisions of the CPC (Articles 225,226, 239 and 240) may be used. While the CPC is used during the investigation phase, the Law on Operational Intelligence Activity of 2007 can be used during the pre-investigation phase.	Article 16 Budapest Convention: Armenia is not in line with Article 16 Budapest Convention. Search and seizure and other powers may be applied to secure electronic evidence but not in an expedited manner. Armenia is cooperating with the Council of Europe to reform the legislation. These reforms should

Party	Legal provisions and practical experience	Assessment
	A preservation order would be possible following a court decision, but this has not been done so far. Regarding international procedures (Article 29 Budapest Convention): A 24/7 point of contact has been established at the Division for High Tech Crime, Main Department Fighting Against Organised Crime in the Police. However, preservation requests cannot be issued. Search, seizure or production orders may be used, but this would require a MLA request followed by a court decision. Thus, there is no experience with international preservation requests.	implement also Article 16. Article 29 Budapest Convention: Armenia is not in line with Article 29. The above reforms should address this.
3. Azerbaijan	Regarding domestic procedures (Article 16 Budapest Convention): No specific legal provisions are available. Other powers (production orders under Article 10 of Law on Investigative Activities, Articles 143.2 (Collection of evidence) and 445 CPC (search, seizure, interception etc.)) are used to obtain data. For procedures under these powers a court order is required (1-2 weeks needed to obtain). However, based on the CPC, which empowers law enforcement to obtain evidence, an agreement has been concluded with service providers. Under this agreement, mobile operators, access and other service providers have appointed "curators" who can be ordered to preserve data in an expedited manner. This arrangement seems to work well in practice. No court order is required for this provisional preservation measure. Regarding international procedures (Article 29 Budapest Convention): The above powers also apply to international requests. International requests may be based on the Law on Mutual Legal Assistance on Criminal Matters (29 June 2001), Budapest Convention on Cybercrime, European Convention on Mutual Assistance in Criminal Matters and other agreements. A 24/7 contact point has been established at the Department of Combating Crimes in	Article 16 Budapest Convention: Azerbaijan is partially in line with Article 16. General investigative powers combined with an administrative agreement with providers allow for the preservation of electronic evidence in an expedited manner if necessary. However, this possibility is not available for legal or physical persons not covered by this agreement. The authorities may therefore want to adopt specific legal provisions. It is understood that the Government intends to reform the Criminal and Criminal Procedure Codes in line with international human rights and rule of law standards. This provides an opportunity to fully implement the procedural law provisions of the Budapest Convention, including conditions and safeguards (Article 15).

Party	Legal provisions and practical experience	Assessment
	Communications and IT Sphere, Ministry of National Security. After receipt of request, the 24/7 CP examines requests (reciprocity, interests of national security etc.), then sends it to Head of General Directorate for Combatting Transnational Organised Crimes who approves execution and forwards it to Cybercrime Unit which interacts with ISP. A formal MLA request is required before collecting and transmitting the data. About 4-5 requests per year are sent or received. The main problem is the limited cooperation received from other countries.	Article 29 Budapest Convention: Azerbaijan is partially in line with Article 29 Budapest Convention. Existing provisions enable to receive and execute MLA requests in an expedited manner. Nevertheless, it is advisable to adopt specific provisions on expedited preservation to broaden the scope beyond service providers and enhance legal certainty.
4. Bosnia and Herzegovina	Regarding domestic procedures (Article 16 Budapest Convention): No specific legal provisions are available at State or entity levels. Art. 72a of the State CPC (and similarly Art. 86a CPC of the Federation of BIH, Art. 137 of CPC of the RS (Official Gazette of RS, No. 53/12) and Art. 72a CPC of Brcko District) allows for "expedited" production orders in urgent cases: A prosecutor or police officer (with the consent of a prosecutor) sends a request to Court which issues a production order. In urgent cases, the prosecutor may order the production of data that remain sealed and informs the judge who may issue the order within 72 hours upon which the seal may be opened. It seems that this possibility is not used very often. Moreover, Article 72a State CPC refers to "information concerning the use of Telecommunication services", that is, to traffic and similar data, but not content. Bosnia and Herzegovina introduced data retention obligations in 2006 by Decision of Council of Ministers of Bosnia and Herzegovina from November 14, 2006 (Official Gazette of Bosnia and Herzegovina, No. 104/06) for a period of 12 months. Regarding international procedures (Article 29 Budapest Convention): Specific provisions have not been adopted but the above Article 72a of the State CPC (and	Article 16 Budapest Convention: Bosnia and Herzegovina is partially in line with Article 16 Budapest Convention. In the absence of a specific legal provision on expedited preservation, the possibility of "expedited production orders" may allow the authorities to secure traffic data held by service providers in an expedited manner. It does not cover content data held by other legal or physical persons. It is advisable that Bosnia and Herzegovina reform its procedural law and adopt specific provisions in line with the Budapest Convention. Article 29 Budapest Convention: Bosnia and Herzegovina is partially in line with Article 29 Budapest Convention, and some requests have been sent and received.

Party	Legal provisions and practical experience	Assessment
	similarly Art. 86a CPC of the Federation of BIH, Art. 137 of CPC of the RS, and Art. 72a CPC of Brcko District) on "expedited production orders" may also be available for international requests for traffic data. In combination with the Budapest Convention or other agreements or the Law on the provision of mutual legal assistance in criminal matters, Article 29 Budapest Convention could be applied for traffic data. A 24/7 point of contact has been established at the International Police Cooperation Sector, Interpol, Sarajevo. A formal MLA request is required for the collection and transmission of data. Based on Article 29 and 30 of the Convention, the Interpol (Directorate for Coordination of Police Bodies) has sent 10 requests to competent authorities of USA and Switzerland, and positive replies have been received.	The application of existing provisions on international cooperation should be promoted. At the same time, it is advisable that Bosnia and Herzegovina adopt specific provisions in line with the Budapest Convention.
5. Bulgaria	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> Preservation orders are possible under the broad powers defined in Article 159 of the Criminal Procedure Code which obliges legal and physical persons to "preserve and hand over" computerised data, including traffic data and other objects that may be of significance to the case. This is ordered by a court or, during pre-trial proceedings, by a prosecutor or the police. It seems that such orders can be obtained rapidly and are issued several times per week. It pertains to all types of data, any crime and any legal or physical person In addition, search and seizure powers may be used. Moreover, data retention is regulated in the Bulgarian Electronic Communication Act. <u>Regarding international procedures (Article 29 Budapest Convention):</u> The powers used for expedited preservation at the domestic level can also be applied for international requests. A 24/7 contact point has been established at the Cybercrime Section, Chief Directorate for Combating Organised Crime, Ministry of the Interior. A request to the 24/7 CP is sufficient to enable a preservation order within one day. About one request is received every two months.	<u>Article 16 Budapest Convention:</u> Bulgaria is in line with Article 16 Budapest Convention. <u>Article 29 Budapest Convention:</u> Bulgaria is in line with Article 29 Budapest Convention.

Party	Legal provisions and practical experience	Assessment
6. Croatia	Regarding domestic procedures (Article 16 Budapest Convention): In Croatia, several provisions are available to permit the preservation of electronic evidence in an expedited manner. These include in particular Articles 261, 263 and 213 of the CPC on the "Temporary Seizure of Objects". A prosecutor, or an investigator or police officer upon his order, can carry out the temporary seizure or issue orders. This relates to any physical or legal person, any type of crime and any type of data. In addition, the power for searches (Article 257.2 CPC), the special collection of evidence (Art. 332, 333 CPC), and confidentiality clause (Art 333.2 CPC) are relevant (special measures can only be taken with respect to a list of serious offences). Moreover, Croatia also adopted data retention obligations (12 months). Regarding international procedures (Article 29 Budapest Convention): The powers used for expedited preservation at the domestic level can also be applied for international requests in combination with agreements such as the Budapest Convention on Cybercrime, the European Convention on Mutual Assistance in Criminal Matters, bilateral treaties, the Law on international legal assistance in criminal matters or the principle of reciprocity. A 24/7 point of contact has been established at the Department for Economic Crime and Corruption, General Police Directorate. A formal MLA request is required for the collection and transmission of data. However, often requests for preservation are not followed by MLA requests.	Article 16 Budapest Convention: Croatia is in line with Article 16 Budapest Convention, although Croatia may consider the adoption of specific provisions. Article 29 Budapest Convention: Croatia is in line with Article 29, although Croatia may consider the adoption of specific provisions.
7. Cyprus	Regarding domestic procedures (Article 16 Budapest Convention): In Cyprus there are no specific provisions on expedited preservation of evidence (electronic or other). However, several provisions are available to permit the preservation of stored computer data which are in the possession or control of the suspect or of any other person.	Article 16 Budapest Convention: Cyprus is partially in line with Article 16 Budapest Convention. Cyprus may consider the adoption of specific legal provisions in line with Article 16 Budapest Convention.

Party	Legal provisions and practical experience	Assessment
	For example, article 6 of the Criminal Procedure Law, Cap. 155, provides for the power of the police to issue production orders of such data either in the possession of the suspect or any other person, during the investigation of any offence. This power relates to all data, apart from those, for the production of which a Court warrant is required (which under the current legislation are the communication data – see below). This is a power largely used by the police and any person who, without reasonable cause, refuses to comply with the police orders given exercising this power, is committing an offence punishable with imprisonment of up to three years. Furthermore, the police has also search and seizure powers that are often used for the preservation of data, which are certainly applied in line with the principle of proportionality (see articles 25-29 and 32-34 of the Criminal Procedure Law, Cap.155). With regard to traffic data, according to Law 183(I)/2007 (which implements Directive 2006/24/EC), all providers of publicly available electronic communications services or of a public communications network are obliged to retain all traffic data, location data and the related data necessary to identify the subscriber or user for a period of six months. According to Directive 2006/24/EC the procedures to be followed and the conditions to be fulfilled in order to gain access to retained data in accordance with necessity and proportionality requirements shall be defined by each Member State in its national law, subject to the relevant provisions of European Union law or public international law, and in particular the ECHR as interpreted by the European Court of Human Rights. The same principles are repeated in the Explanatory Report on the Convention on Cybercrime. Therefore, because of the sensitivity of those data, and in accordance with our Constitution (Article 17), Law 183(I)/2007 provides that the Police can gain access to those data, for the purpose of the investigation of offences, based on a Court warrant and only regarding offences punishable with imprisonment of at least five years. However, all offences under the Convention on Cybercrime are punishable with imprisonment of at least five years. On the other hand, access to traffic data that may represent electronic evidence in relation to offences that are not serious would be difficult. The adoption of specific preservation provisions would allow Cyprus to secure electronic evidence while at the same time respecting rule of law and human rights requirements.	<u>Article 29 Budapest Convention:</u> Cyprus is partially in line with Article 29 Budapest Convention. Cyprus may consider the adoption of specific legal provisions in line with Article 29 Budapest Convention.

Party	Legal provisions and practical experience	Assessment
	Regarding international procedures (Article 29 Budapest Convention): The same powers available at the domestic level can be applied for international requests, since Article 3.3 of the Law 22(III)/2004 (which is the implementing legislation of the Convention on Cybercrime in Cyprus), provides that Law 23(I)/2001 (Law on International Cooperation on Criminal Matters) is applicable regarding international requests based on the Convention on Cybercrime. Article 9.9 of Law 23(I)/2001 provides that all the powers of the Police under the Criminal Procedure Law, Cap.155, are available for the execution of international requests. With regard to traffic data the above limitations apply. A formal international request is required for the above procedure to commence. A request containing the information listed in Article 29.2 Budapest Convention would be sufficient. Upon receipt by the 24/7 contact point, it is sent to the Ministry of Justice for verification and onward transmission to competent authorities within Cyprus. This approach risks delaying the execution of international preservation requests. The role of the 24/7 contact point seems more limited than what is foreseen in Article 35 Budapest Convention. Specific preservation provisions may allow for a more efficient approach to the securing of electronic evidence upon an international request.	
8. Denmark	[Denmark did not reply to the questionnaire]	Article 16 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision. Article 29 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision.

Party	Legal provisions and practical experience	Assessment
9. Estonia	Regarding domestic procedures (Article 16 Budapest Convention): Estonia has not adopted specific provisions on expedited preservation. However, the general powers of § 215 CPC may be used that obliges anybody to comply with orders and demands of investigative bodies and prosecutors' offices. In most cases, direct search, seizure and production orders rather than provisional measures are applied in line with principles of necessity and proportionality. Traffic and subscriber data is retained by providers under the Electronic Communications Act (§ 111 – 113). Disclosure of traffic data is permitted only with regard to serious criminal offences (sanction must be at least 3 years imprisonment). This means that there are stricter hurdles to the disclosure of traffic data than for content data. Cooperation agreements have been concluded with major providers regarding request and submission of data. Regarding international procedures (Article 29 Budapest Convention): Specific legal provisions for preservation have not been adopted, but other powers – to some extent – can be used at the domestic level to secure electronic evidence. A 24/7 point of contact has been established. However, the powers available are not applied for international preservation requests and there is no practical experience.	Article 16 Budapest Convention: Estonia is partially in line with Article 16 Budapest Convention. Expedited preservation is not used in practice. Estonia may consider the adoption of specific provisions on expedited preservation and promote their use in practice. New legislation will enter into force on 1 January 2013. According to the amendments to the Criminal Procedure Code, preservation and disclosure of data (including traffic data) will be allowed with regard to any criminal offence. Article 29 Budapest Convention: Estonia is partially in line with Article 29 Budapest Convention, but not used in practice. Estonia may consider the adoption of specific provisions.
10. Finland	Regarding domestic procedures (Article 16 Budapest Convention): Finland adopted a specific provision on expedited preservation in Chapter 4, Section 4b and 4c of the Coercive Measures Act (450/1987) as amended in 2007 (this corresponds to Chapter 8, Sections 24-26 in the reformed Coercive Measures Act (806/2011). In practice, however, seizure provisions are used to obtain data with respect to domestic investigations. This provision covers any data, in relation to any offence and any physical or legal person holding data.	Article 16 Budapest Convention: Finland is in line with Article 16 Budapest Convention. Article 29 Budapest Convention: Finland is in line with Article 29 Budapest Convention although the provision has not yet

Party	Legal provisions and practical experience	Assessment
	Moreover, Finland adopted data retention regulations. Regarding international procedures (Article 29 Budapest Convention): The above measure can also be applied for international requests. General grounds for refusal to provide assistance are listed in Sections 12 and 13 of the Act on International Legal Assistance in Criminal Matters (4/1994) (prejudice to sovereignty, security, essential interests; contrary to principles of human right or ordre public; political offence and similar). Act (4/1994) is a general MLA law which can be applied also in relations with non-contracting parties. Therefore it is worth noting that this general MLA law also has a provision (§30) which states that regardless the provisions of this law Finland provides assistance as specifically agreed e.g. in international Conventions.	been tested in practice.
11. France	Regarding domestic procedures (Article 16 Budapest Convention): Article 56-7 and Article 60-2 of the CPC are used to secure electronic evidence in an expedited manner through preservation or seizure. This applies to any data and any offence. Article 60-2 CPC is used for service providers. The measures are carried out by the judicial police upon the order of a prosecutor. Specific templates are used for preservation requests. Moreover, France adopted data retention regulations. Regarding international procedures (Article 29 Budapest Convention): The powers to secure electronic evidence through preservation or seizure in an expedited manner at the domestic level are also applied for international requests. Requests are usually received by 24/7 contact point by email and checked for completeness (if necessary additional information is sought from the requesting CP). Receipt is confirmed. A request is sent by the CP to the service provider using a specific template. Upon reply by the service provider the requesting CP is informed and asked to send a formal rogatory letter to obtain the data.	Article 16 Budapest Convention: France is in line with Article 16 Budapest Convention. Article 29 Budapest Convention: France is in line with Article 29 Budapest Convention.

Party	Legal provisions and practical experience	Assessment
	The Office Central de Lutte contre la Criminalité Liée aux Technologies de l'Information et de la Communication (OCLCTIC) de la Direction Centrale de la Police Judiciaire is the 24/7 contact point that orders providers to preserve at the request from abroad. An MLA request is needed to produce and release the data. Some 3-5 requests are sent/received per month. Preservation orders are issued within 24 hours. The procedure is considered efficient. Problems: ▪ No uniform templates and procedures for incoming requests ▪ Preservation request often not followed by MLA requests for data ▪ Missing relations with bodies responsible for MLA to support follow up through judicial cooperation.	
12. Georgia	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> No specific provisions for expedited preservation have been adopted but search, seizure and production orders (Articles 111, 112, 119, 120 or 136 CPC) as well as "operative-investigative activity" are applied. The main provision is Article 136 on production orders which is frequently used in practice The condition for production orders and other powers is "probably cause". The "probable cause" is the lowest in the hierarchy of evidentiary standards as prescribed by the Criminal Procedure Code of Georgia and is the standard generally used for bringing initial charges against defendants in criminal cases. A Memorandum of Understanding between law enforcement agencies and service providers was signed in May 2010. Public/private cooperation on the basis of this MoU appears to function very well. It appears that the standard of "probably cause" in Georgia is sufficiently low to allow for efficient use of production orders. Article 3 (definition of terms), par. 11 states the following: "Probable Cause - a body of information or facts that in corroboration with all circumstances of a given criminal case would be sufficient for the reasonable person to conclude that a person has probably committed a crime; an evidential standard for conducting investigative activities directly prescribed by this Code and/or imposing	<u>Article 16 Budapest Convention:</u> Georgia is partially in line with Article 16 Budapest Convention. The combination of search, seizure and production orders on the one hand, and cooperation with service providers on the basis of a MoU on the other seems to allow securing electronic evidence in an expedited manner. Georgia may nevertheless wish to consider the adoption of specific expedited preservation provisions. <u>Article 29 Budapest Convention:</u> Georgia is partially in line with Article 29 Budapest Convention. According to information provided a new law on international enforcement cooperation is in

Party	Legal provisions and practical experience	Assessment
	preventive measure". Regarding international procedures (Article 29 Budapest Convention): As indicated, in the absence of specific provisions, other powers may be used to secure electronic evidence in an expedited manner at the domestic level. The statute of the newly created Specialised Cybercrime Unit of Central Criminal Police Department gives this unit the responsibilities of a 24/7 point of contact, including international cooperation to secure data in line with Article 29 without the need for mutual legal assistance. So far, no requests have been sent or received.	preparation and will fully reflect the requirements of Article 29.
13. Germany	Regarding domestic procedures (Article 16 Budapest Convention): No specific provisions for expedited preservation have been adopted. Provisions on the retrieval of subscriber data, on securing and seizure and on the collection of traffic data allow to "similarly obtain" the securing of data as permitted under Article 16 Budapest Convention. This has shown to work in practice. A request for identification of the subscriber behind a dynamic Internet Protocol address, which is especially relevant in practice, is responded to in Germany in the form of so-called "subscriber data disclosure" (Bestandsdatenauskunft). This does not require judicial authorisation and is not limited to specific criminal offences. Under the applicable law, the prosecution authorities are entitled to demand disclosure of subscriber data (such as the name and address of the subscriber, telephone numbers allocated and other connection labels) pursuant to the general clause on investigations (sections 161 (1), first sentence, 163 of the Code of Criminal Procedure (CCP) in connection with section 113 (1) of the Telecommunications Act). The only requirement is that the collection of the subscriber data is necessary for the prosecution of a criminal offence in respect of which criminal proceedings have been instituted. An authorisation by the court or the public prosecution office is not necessary. In addition, the Convention is implemented both by the provisions on securing and seizure in general (sections 94 et seqq. CCP) and by the provisions on the collection of traffic data	Article 16 Budapest Convention: Germany is in line with Article 16 Budapest Convention in that alternative means to secure evidence in an expedited manner are available and used in practice. However, Germany may wish to consider the adoption of specific expedited preservation provisions for domestic and international procedures. This may make the system less complex and more predictable. Article 29 Budapest Convention: Germany is in line with Article 29 Budapest Convention in that alternative means to secure evidence in an expedited manner are available and used in practice. However, Germany may wish to consider the adoption of specific expedited preservation provisions for domestic and international procedures. This may simplify

Party	Legal provisions and practical experience	Assessment
	(section 100g CCP), which allow for the expeditious preservation of traffic data while taking into account the principle of proportionality. Seizures require a court order as a matter of principle. However, seeking a court order is possible in an expedited manner. Courts provide an on call service which rotates between judges and which is now organised in such a way that a court order can be obtained on very short notice. The same is true for the prosecutors' offices and the police which are available 24/7. If in exceptional circumstances it should not be possible to obtain a court order fast enough, an order by a public prosecutor or (if traffic data is not concerned) by the police is sufficient. So if prosecutor and police believe that data could be deleted any moment, they do not need to apply for a court order, but can and must act by themselves under such exigent circumstances and are entitled to order seizure to secure the data. These seizure provisions may apply to all crimes and to any legal or physical person. For traffic data stored by a provider, Section 100g CCP can be used. The principle of proportionality applies and thus there are limitations regarding access to such data. Law enforcement can obtain traffic data in cases where a criminal offence of substantial significance in the individual case has been committed. While the German authorities consider that these limitations are permitted under Article 15 on conditions and safeguards, it may not always be possible to determine at the outset whether an offence is serious in nature. Under this provision it would thus not be possible to ensure the preservation of data in order to evaluate the situation. However, traffic data can also be obtained where a criminal offence has been committed by means of telecommunication – irrespective of whether or not it is a serious or a petty offence. This provision would, for example, apply in all cases, where emails, phone calls or the internet are used for an offence, for example when committing online fraud. Thus, only when it comes to the very narrow area of petty offences not committed by means of telecommunication, traffic data stored by a provider cannot be obtained by law enforcement. As in the case of seizure a court order is required as a matter of principle. However, in exigent circumstances a prosecutor can order the measure.	international cooperation.

Party	Legal provisions and practical experience	Assessment
	A specific preservation provision is found in Section 16b of the Act on Securities Trading. It relates to traffic data in cases of suspected insider trading or market manipulation. In Germany, traffic data is not retained without a specific suspicion ("anlasslos") since the law implementing the EU Data Retention Directive was declared non-constitutional in 2010. However, telecommunications services providers continue to retain traffic data on the basis of Sections 96 et seq. of the Telecommunications Act, notwithstanding the decision of the Federal Constitutional Court. These data may be obtained as before. While this system is applied in practice is appears to be rather complex considering also the federal structure of Germany. The different layers risk resulting in delays and a level of unpredictability. <u>Regarding international procedures (Article 29 Budapest Convention):</u> In the absence of specific legal provisions on expedited preservation, search and seizure provisions and the Law on international legal assistance (IRG) may be used. Section 74 provides for the possibility that the Ministry of Justice delegates responsibility for international requests to other Federal or State level agencies. Section 67 IRG covers search and seizure and may thus be used to secure electronic evidence. A court order is required, but in emergency cases, i.e. when lodging an application with a court carries the risk that evidence may be lost a prosecutor may order the search and seizure. Section 67(1) stipulates that search and seizure may already be carried out prior to the receipt of the formal rogatory letter. A request meeting the formal requirements of Article 29.2 Budapest Convention would be sufficient to secure data in Germany. A request for mutual assistance is needed for the disclosure of data to foreign authorities. A 24/7 single point of contact has been established at the National High Tech Crime Unit, Federal Criminal Police Office (BKA). In general, the contact point is authorised to send/receive and follow up to requests for preservation. In the context of the international	

Party	Legal provisions and practical experience	Assessment
	procedures (Art. 29 of the Convention), the contact point serves as a first port of call for the submission of a preservation order to the competent judicial or police authorities and to initiate further steps. While Germany has been successfully cooperating with other Parties in numerous cases, the system appears to be rather complex and difficult to understand for foreign counterparts.	
14. Hungary	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> Article 158/A CPC allows for the expedited preservation of any computer data. A preservation order is issued by court, a prosecutor or the investigating agency and is valid for a period of up to three months. In practice, this procedure is considered complicated and is open to complaints and judicial control. Therefore, general powers to obtain data through production orders or search or seizure are used more often. In addition, cooperation agreements have been signed with service providers. Data retention regulations have been adopted. <u>Regarding international procedures (Article 29 Budapest Convention):</u> For international requests, Hungary needs to open its own investigation before preserving data. Often arrangements with providers are therefore used to preserve data. The International Law Enforcement Cooperation Centre of the Police serves as 24/7 point of contact. The alternative contact point is the High-tech Crime Unit of the National Bureau of Investigation.	<u>Article 16 Budapest Convention:</u> Hungary is in line with Article 16 but may consider steps to facilitate application of the preservation provision in practice. <u>Article 29 Budapest Convention:</u> Hungary is partially in line with Article 29. Preservation through Article 158/A is complex and not possible without a domestic investigation. So far, the provision has not been applied in practice. Other arrangements and powers therefore need to be used. Hungary may consider the adoption of specific provisions.

15. Iceland	[Iceland did not reply to the Questionnaire]	Article 16 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision. Article 29 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision.
16. Italy	Regarding domestic procedures (Article 16 Budapest Convention): Through Law 48 of 18 March 2008, a number of Articles were modified in or added to the Code of Criminal Procedure which provide for urgent measures to secure electronic evidence. These include Article 244 (inspections permitting the preservation of data), 247 (searches permitting also the preservation of data), 248 (production orders), 254 (seizure of correspondence), 254bis (which includes preservation orders to service providers), 259 (custody of things seized, including of data preserved), 352 (searches, including technical measures to preserve data), 354 (urgent investigations and seizure, including securing of data and computer systems). In urgent cases or in flagranti these measures can be taken by the judicial police or ordered by the prosecutor immediately. They apply to all types of data and to any physical or legal person. Regarding international procedures (Article 29 Budapest Convention): [no information received]	Article 16 Budapest Convention: Italy is in line with Article 16. Article 29 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision.
17. Latvia	Regarding domestic procedures (Article 16 Budapest Convention): Section 191 CPC is a specific provision for expedited preservation. The procedure is that an investigator (for instance, Cybercrime combating and IPR protection unit) prepares the decision based on Criminal procedure law Chapter 191.	Article 16 Budapest Convention: Latvia is in line with Article 16. Article 29 Budapest Convention:

	At the same time the investigator communicates with the service provider and visits the particular location (service provider data storage technical room), where the data has to be preserved. The investigator controls the preservation procedure and the hashsum calculation. This provision can be used for any type of investigation relevant data. An ISP could be liable in case of disclosure of information on investigation. <u>Regarding international procedures (Article 29 Budapest Convention):</u> For international requests the following procedure is applied: ▪ The 24/7 Contact Point (International Cooperation Bureau of the Central Criminal Police department) receives the request and forwards it to Cybercrime Combating and IPR Protection Unit ▪ The Unit communicates with initiator specifying particular needs and required information to be preserved ▪ The Unit prepares a request based on Criminal procedure law and Convention ratification law; ▪ At the same time, the Unit communicates with service provider and goes to particular location (service provider data storage technical room), where the data has to be preserved ▪ The Unit controls the preservation procedure and the hashsum calculation ▪ After preservation is completed, the Unit notifies the 24/7 Contact Point at the State Police. About 2 requests are received per month by the 24/7 point of contact. Preservation requests are usually executed within one day. Traffic data can be shared internationally, for content a MLA request is required. The strength is the cooperation with service providers. The absence of a specific legal provision in the CPC on international preservation orders is considered a problem.	Latvia is in line with Article 29 Budapest Convention.

18. Lithuania	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> Several provisions are used for preservation or otherwise securing electronic evidence. These include in particular Article 155 CPC (right of a prosecutor to become familiarised with information). Once a pre-trial investigation is started, the procedure of Article 155 is followed: The investigating officer shall apply to the leading prosecutor to get his approval to make a request for data preservation. If a prosecutor approves, he passes a decision, which should be approved by pre-trial investigation judge. When all requirements provided by law are fulfilled, the request is submitted to the head (or other competent official) of the relevant undertaking providing electronic communications networks and/or services and the actions needed are taken. Search and seizure powers (Article 147 CPC) are also available. Lithuania introduced data retention under the Law on Electronic Communication of 15 April 2004 for serious crime. Information can furthermore be requested under the Law on Police Activities of 2000. In addition, Article 10 of the Law on Operational can be used to obtain information. Finally, agreements between police and main providers enable access to data. In practical terms it appears, therefore, that because of data retention or powers to seize, search or inspect and others, expedited preservation is not used at the domestic level. <u>Regarding international procedures (Article 29 Budapest Convention):</u> Article 67 § 5 CPC provides that "in cases provided for in an international agreement to which the Republic of Lithuania is a party, the courts, institutions of prosecution and pre-trial investigation shall execute the requests of institutions of foreign states received directly and shall directly transmit to foreign states replies to their requests." International preservation requests under Article 29 Budapest Convention can thus be executed. Per Order of Police Commissioner General No. 5-V-1102, 12 December, 2011: 24/7 CP can sent/receive directly requests for preservation from foreign contact points. The Lithuanian contact point has been established at the Cybercrime Unit, Lithuanian Criminal Police Bureau.	<u>Article 16 Budapest Convention:</u> Lithuania is partially in line with the Budapest Convention. In principle, preservation is possible but the procedure appears complex and is not used in practice. Lithuania may wish to consider the adoption of specific expedited preservation provisions for domestic and international procedures. (The T-CY was informed that amendments are underway.) <u>Article 29 Budapest Convention:</u> Lithuania is partially in line with Article 29 Budapest Convention, although the system has not yet been tested successfully. The actual use of international preservation requests should be promoted.

	Lithuania has received a number of requests from abroad but without confirmation that the requesting Party intended to send an MLA request subsequently (as foreseen in Article 29.2f). The requests were therefore not executed.	
19. Republic of Moldova	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> Article 7 of the Law on Preventing and Combating Cybercrime (Law nr. 20-XVI of 03/02/2009) obliges service providers to preserve computer data upon request for up to 120 days. Such requests can be issued in relation to any crime. The request is issued by a prosecutor. A template is used. A court order is required for the subsequent production of data. This measure is often used and considered essential for investigations. <u>Regarding international procedures (Article 29 Budapest Convention):</u> Article 10 of Law 20-XVI of 03/02/2009 implements in the national legislation Article 29 of the Budapest Convention. According to Article 10 a foreign authority can ask for expedited preservation of computer data (content) and traffic data to the Moldavian authorities. Both 24/7 contact point within the General Prosecutor Office and the one within the High-tech Crime Unit are authorised to order preservation against any entity (natural or legal person). Written requests are required for preservation. The data is collected based on a resolution issued by the General Prosecutor's Office and a judge order. The transmission of the data is done by mutual legal assistance request; there for the preservation order cannot be issued for less than 60 days. About 20 requests are sent/received per month according to information provided.	<u>Article 16 Budapest Convention:</u> Moldova is partially in line with Article 16 Budapest Convention. Article 7 of the Law on Cybercrime is limited to service providers. Unless other powers are available allowing ordering of any physical and legal person to preserve data, the scope of Article 7 should be broadened. <u>Article 29 Budapest Convention:</u> Moldova is in line with Article 29 Budapest Convention since for international requests preservation is not limited to service providers.

20. Montenegro	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> Montenegro does not have a specific provision on expedited preservation but search and seizure (Article 75 CPC) and the provisional/temporary seizure (Article 85 CPC which includes electronic data) may be used. If a search is needed the order is issued by the Court at the request of the State Prosecutor or at the request of the police officer who received the approval of the State Prosecutor. The request is submitted in written form and it can be submitted orally as well (reasons of urgency, telephone request submitting, Article 76 of the CPC). The order is issued by the investigative judge (written form). If needed, the procedure can be completed very quickly. For example, if a police officer with the approval of the prosecutor after a telephone conversation calls the investigative judge and requests issuance of the order, such an order can be issued by the judge immediately. In case of the provisional (temporary) seizure of objects referred to in Article 85 of the CPC the prosecutor will send a written proposal and the court will issue a decision emphasizing from who the objects (electronic data) should be seized from and that they have to be submitted in a legible and comprehensible form to the Court for preservation or their preservation shall be provided in some other way (for example, order to the Internet provider to preserve such data within their technical capacities and to provide them at the request of the Court). In practical terms, preservation is rarely used. <u>Regarding international procedures (Article 29 Budapest Convention):</u> The powers to secure electronic evidence at the domestic level (search, seizure, temporary seizure) can also be applied for international preservation requests. The difference is that in this case the 24/7 contact point at the Police Directorate of Montenegro is the person who contacts the State Prosecutor with the request to send the judge the request for investigation, to issue the search warrant or a proposal for provisional (temporary) seizure of objects. The contact person will refer to Articles of the Budapest Convention when explaining the need for such a request and all the procedure remains the same. So far, however, no requests have been sent or received.	<u>Article 16 Budapest Convention:</u> Montenegro is in line with Article 16 Budapest Convention although specific provisions should be considered and practical application should be promoted. <u>Article 29 Budapest Convention:</u> Montenegro is in line with Article 29 Budapest Convention, although the system has not yet been tested. The actual use of international preservation requests should be promoted.

21. Netherlands	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> A specific provision is available with Article 126ni of Dutch Code of Criminal Procedure. The procedure is described in article 126 ni DCCP itself. The request is delivered by the prosecution office either orally or in writing. When delivered orally, a written version is to be transferred to the requested party within 3 days and is signed by a prosecutor. The written request stipulates: a. An accurate description of the data to be preserved; b. Date, time of request c. The grounds that justify the request d. The period of requested preservation e. Whether the request also involves data necessary for retrieving the identity of other providers whose networks or services were used in the relevant communication. The public prosecutor makes a report on his request. The measure is available for crimes for which pre-trial detention is possible. <u>Regarding international procedures (Article 29 Budapest Convention):</u> Article 126ni of DCCP for domestic preservation may also be used for international requests. The public prosecutor is competent for receiving and executing request. The prosecutor needs to be convinced that there are grounds for a request for preservation. The public prosecutor for cybercrime "directs" the national high tech crime unit. The HTCU is the focal point (24/7) for cybercrime and will contact partners in order to have a preservation order "served" to another state (via that state's point of contact). The provision is used frequently, in particular at the international level.	<u>Article 16 Budapest Convention:</u> The Netherlands is in line with Article 16 Budapest Convention. <u>Article 29 Budapest Convention:</u> The Netherlands is in line with Article 29 Budapest Convention.

22. Norway	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> A specific provision is available in Section 215a Criminal Procedure Act. It can be used for any data and for any offence while the principle of proportionality is to be respected. The prosecutor in charge of the case signs a document addressed to the company that is required to secure the data in question; then the police officer in charge of the case contacts the company, usually by phone, and the request is sent to the company by e-mail or fax. Usually, the company will send a confirmation by e-mail or fax shortly after, confirming that the data in question has been secured for the time period in question. If the police do not receive a confirmation, the company will be contacted again to make sure that the request for data preservation is processed. Data retention is not yet available in Norway, and this is considered a major problem as preservation or production orders often arrive too late when data is no longer available. (A data retention regulation is pending entry into force). <u>Regarding international procedures (Article 29 Budapest Convention):</u> The specific provisions for domestic preservation can also be applied for international requests. In fact, preservation is primarily used with respect to international requests, while within Norway most often production orders are issued. The provision is thus considered important for international cooperation. In the majority of cases, the international preservation requests will be handled by NCIS Norway (Kripos). NCIS Norway is also the international contact point for G8, Interpol and Europol. When a request has been received, the prosecutor in charge of the case will sign and order for expedited preservation of data, in accordance with the Criminal Procedure Act Section 215a. The police officer in charge of the case will then contact the company that has the data in question, to present the document, ask for confirmation that the data will be preserved, as well as contact information for the people in responsible for securing the data. When this is done, the police will inform the party who requested the data preservation that their request has been processed. This information is often given by e-mail. No statistics available but preservation orders are usually issued the same or following	<u>Article 16 Budapest Convention:</u> Norway is in line with Article 16 Budapest Convention. <u>Article 29 Budapest Convention:</u> Norway is in line with Article 29 Budapest Convention.

	business day. The main strength is considered that preservations can be ordered rapidly. The main problem is to actually obtain the data.	
23. Portugal	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> A specific provision is available in Article 12 of the Law on Cybercrime (Law nº 109/2009, from 15 September). Written preservation order issued by prosecutor or in urgent cases by police. The letter with the order of preservation must describe the nature of the data that should be preserved, the origin and destination of those data, if known (in case of traffic data), and the period of time covered by the preservation order. There is a limit of three months, as maximum, to that period. However, the order can be renewed for periods of time according to that limit, up to a maximum of one year. After the issue of the order, the ISP (or whoever has availability or control over the data), preserves immediately the data concerned and waits until the end of the term of the order the arrival of a proper seize or disclosure order. If this last one does not arrive, the preservation order expires and the data are destroyed. Data retention is regulated in a separate law (No 32/2008). <u>Regarding international procedures (Article 29 Budapest Convention):</u> Specific provisions for international preservation request are available in Articles 22 and 23 of the Law on Cybercrime (Law nº 109/2009). Article 22 refers to procedure of preservation and Article 23 is about grounds for refusal. The contact point in the Judicial Police has competence for receiving and executing international preservation request. A request must meet the requirements of Article 22 of the Law on Cybercrime and must mention the intention to submit a formal request for assistance for search, seizure and disclosure of the data. This request must be sent by the requesting country to Polícia Judiciária that will forward it to the judicial authority. The judicial authority will issue an order of preservation to the person who has the control or availability of such data. Polícia Judiciária can also issue the	<u>Article 16 Budapest Convention:</u> Portugal is in line with Article 16 Budapest Convention. <u>Article 29 Budapest Convention:</u> Portugal is in line with Article 29 Budapest Convention.

	order when there is an emergency or danger in delay, reporting it to the prosecutor immediately. Frequent requests are received by the 24/7 contact point outside office hours for different types of assistance and information. These are not always labelled "preservation requests".	
24. Romania	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> A specific provision is available in Article 54 of Law 161/2003. This covers any data, any type of crime and any type of physical or legal person holding data. Regarding the scope of procedural law provisions of the above law (Article 58), jurisprudence has given a broader interpretation of Article 58. If one or several material acts of a crime are committed by means of computer system, or evidence of such an act is stored or was transmitted through computer systems, provisions related to preservation, computer search, interception of a computer communication are applicable. In terms of procedures, whenever there is a danger for the data to be lost, ex officio or upon judiciary police's request, the prosecutor will issue the order for expedited preservation and will send it to the provider or to the specific person who has the data. During the trial the judge will assume such an order ex officio or upon the participants' request (prosecutor, injured party other participants). The receiver of the order has the obligation to set up necessary measures to preserve the data/traffic data, keeping confidentiality and using proper techniques to ensure the integrity of the data/traffic data. At the end of the measure (90 days, extension 30 days) or within this period the preserved data are to be released to the prosecutor upon a subsequent order (authorization) issued by the prosecutor. The authorization contains the obligation for the provider to put at the prosecutor disposition the equipment containing the preserved information in order to make copies. In case the provider or the person fails to comply, the prosecutor will submit a mandatory order to surrender the equipment which will be executed by himself or by the judiciary police. Preservation orders are considered important but are not used that frequently at the domestic level, as most requests are for information related to IP addresses.	<u>Article 16 Budapest Convention:</u> Romania is in line with Article 16 Budapest Convention. <u>Article 29 Budapest Convention:</u> Romania is in line with Article 29 Budapest Convention.

	Informal cooperation arrangements between law enforcement and service providers facilitate cooperation. <u>Regarding international procedures (Article 29 Budapest Convention):</u> Specific provisions for international preservation request are available in Articles 63 and 64 of Law 171/2003. Requests are most of the time received via email. They are registered and dealt with immediately or the following working day, usually by the Prosecutor at the Service for Countering Cybercrime. In all cases the prosecutor will briefly verify the information received (if the provider was correctly identified, if there is a valid time stamp etc.) and will issue the ordinance. If the information is not accurate the prosecutor will ask for its rectification. The ordinance is sent to the provider and the foreign authority will be informed accordingly. They will also be notified that for retrieval of data a rogatory letter will be required. Usually the ordinance is issued for a period of 90 days. The prosecutor will inform the foreign authority if the time expires without receipt of a rogatory letter. When a letter rogatory has been received, the prosecutor will proceed as for a domestic measure, respectively the prosecutor will issue an authorization for retrieval the information that was preserved and the provider has the obligation to put at prosecutor's disposition the equipment in order to make copies. Finally, the information is sent to the foreign authority via international cooperation channels. Note: If the preservation request is asking for computer data held by a natural person, the foreign authority will be informed about the risk of serving the order. The foreign authority will be informed about the person, location or other relevant information. Such a notification will be sent in all cases for which Romanian LEA information points at the risk that the other country's investigation could be jeopardised (small service providers). Sometimes a production order is sent to service providers if it is clear from the foreign request that only subscriber information is needed for further assessment/request. During the past few years Romania received 10 to 15 international preservation requests per year. The main problem is that not all of them are followed by MLA request or a note saying the	

	information preserved is no longer needed, since the related MLA process is considered too complex.	
25. Serbia	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> Serbia does not have a specific provision on expedited preservation but Article 85 (1), Article 146 and Article 255 (2) can be used. When needed a law enforcement officer, a prosecutor or court, depending on the phase of the criminal proceedings, issues a request or order to the entity to preserve specific stored data until production or search and seizure order has been issued. Preservation is used if a search, seizure or production order is not immediately available. It is used for banks, insurance companies and other private sector entities holding databases, that is, not only for ISPs. Preservation is possibly for any data and offence. In cases of serious crime additional measures are available. The data retention obligation offers additional possibilities to secure electronic evidence. <u>Regarding international procedures (Article 29 Budapest Convention):</u> The powers and procedures to secure electronic evidence are also applied for international preservation requests. The competence for sending/receiving requests is with the Ministry of Interior, the Republic's Prosecutor Office, the Special Prosecutors Office for High-tech Crime and Courts. A 24/7 point of contact has been established at the Cyber Crime Department, Service for Combating Organized Crime, Ministry of Interior and an alternative one at the Republic's Public Prosecutor's Office. International preservation requests are not used very often because of the complicated follow up through MLA.	<u>Article 16 Budapest Convention:</u> Serbia is in line with Article 16 Budapest Convention although specific provisions should be considered. (The T-CY was informed that proposals for amendments are under discussion). <u>Article 29 Budapest Convention:</u> Serbia is in line with Article 29 Budapest Convention. The actual use of international preservation requests should be promoted. The adoption of specific provisions on expedited preservation should be considered (see comment on Article 16). Note: a new CPC is to enter into force in 2013.

26. Slovakia	Regarding domestic procedures (Article 16 Budapest Convention): With Section 90 (Preservation and Disclosure of Computer Data) a specific provision was introduced in the Code of Criminal Procedure. It covers physical and legal persons and all types of data. The preservation order can be issued by a prosecutor without court order. The measure is often used. Regarding international procedures (Article 29 Budapest Convention): Section 90 CPC can also be used to execute an international preservation order. Letters rogatory are required for the disclosure of data to foreign authorities (Section 537 ff of the Code of Criminal Procedure). The National Central Bureau Interpol serves as 24/7 Contact Point and is competent to send/receive requests (about 60 requests per year).	Article 16 Budapest Convention: Slovakia is in line with Article 16 Budapest Convention. Article 29 Budapest Convention: Slovakia is in line with Article 29 Budapest Convention.
27. Slovenia	Regarding domestic procedures (Article 16 Budapest Convention): Slovenia does not have specific provisions on expedited preservation but the following CPC articles are being used by LEA and Public Prosecution to secure data: • Article 148 is a general provision, which requires the police to protect (i.e. preserve) traces and objects (i.e. digital data) which may be evidence (i.e. digital evidence) • Article 149b refers to the obtaining of traffic data from telecommunications operators via a court order • Article 150 which is a special provision for lawful interception • Article 164 which is a general provision that allows police to seize items (i.e. digital evidence) and do a house and/or personal search, • Article 220 which allows the police to seize (also temporary) items (i.e. digital items) In practice, there are 3 possibilities: • The first is that police acts under Article 148 CPC and inform user/owner of digital evidence to preserve it. That is usually done via phone call or e-mail often followed by official letter. This can be done in a short time - not more than one hour. • The second way is that if the user/owner of digital evidence is not cooperative or if so	Article 16 Budapest Convention: Slovenia is partially in line with Article 16 Budapest Convention. The adoption of specific provisions should be considered. Article 29 Budapest Convention: Slovenia is partially in line with Article 29 Budapest Convention. The adoption of specific preservation provisions should be considered. The use of current provisions for international cooperation should be promoted.

	decided by the police (e.g. for future need of partial disclosure) the police can seize (also temporarily) digital evidence in under Articles 164 and 220. This can also be done in a short time, not more than 3-4 hours. • The third way is for the police to obtain a court order (from an investigative judge) for seizing digital evidence and then seize it. When the court order is issued then the user/owner must disclose the digital evidence. This can be done within 24 hours (usually within one working day). <u>Regarding international procedures (Article 29 Budapest Convention):</u> These three ways and the CPC Articles mentioned above for expedited preservation at the domestic level can also be used with respect to international requests. They can be used for any subject (person, institution, private/public company or organisation) and any type of crime. Article 515 of CPC regulates International cooperation with regards to article 29 and allows police/prosecutor/judge to provide direct assistance to other law enforcement agencies and with the use of i.e. e-mail or similar. The Sector for international police cooperation, Criminal Police Directorate serves as the 24/7 point contact. The Cyber Investigation Unit of the Criminal Police Directorate serves as alternative contact point. International requests are received by the Sector for International Police Cooperation. The further procedure is same as for Article 16. Slovenia has only received 2-3 requests so far and never sent any.	
28. Spain	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> According to the replies received, Spain has adopted data retention regulations in line with the EU Directive covering traffic data and subscriber information and pertaining to service providers, but no provisions for expedited preservation in the sense of Article 16 Budapest Convention are available. According to jurisprudence access to retained traffic data is possible in relation to any crime committed by means of computer networks.	<u>Article 16 Budapest Convention:</u> Spain is not in line with Article 16 Budapest Convention. The data retention regulations referred to in the replies do not meet the requirements of Article 16.

	Regarding international procedures (Article 29 Budapest Convention): Provisions allowing to execute international preservation requests are not available.	It is understood that a revision of the Spanish Criminal Procedure Code is currently under consideration. This offers an opportunity to fully implement Article 16. Article 29 Budapest Convention: Spain is not in line with Article 29 Budapest Convention.
29. Switzerland	Regarding domestic procedures (Article 16 Budapest Convention): Switzerland does not have specific provisions on expedited preservation. Seizure and production orders (Articles 263-266) can be used to secure electronic evidence in an expedited manner. These formal powers are supplemented by an informal agreement between law enforcement and major Internet service providers which refers to the preservation of data. Preservation orders may thus be issued by the authority leading an investigation at a given stage, that is, the police, the prosecutor or a judge. This arrangement has proven to function in practice as long as the officer or prosecutor in charge is familiar with the procedure. Regarding international procedures (Article 29 Budapest Convention): According to article 18 of the Swiss Law on Mutual Legal Assistance, provisional measures (such as securing data) may be taken by the competent Swiss authorities in order to - protect and safeguard threatened legal interests - preserve the existing situation and to - protect evidence at risk of loss. These steps may be taken as soon as the request is announced and under the conditions that - the proceedings do not appear to be in admissible or inappropriate - there is sufficient evidence which indicates the need to act on an provisional basis	Article 16 Budapest Convention: Switzerland is in line with Article 16 Budapest Convention. Article 29 Budapest Convention: Switzerland is in line with Article 29 Budapest Convention.

	- the case is not considered a minor case which would not justify conducting proceedings. Finally, measures will be revoked and data will not be handed over to the requesting foreign authorities in cases where, subsequently, the formal request is not made within the deadline set.	
30. "The former Yugoslav Republic of Macedonia"	<u>Regarding domestic procedures (Article 16 Budapest Convention):</u> The temporary seizure foreseen in articles 203 to 206 of the (current) CPC may be used to secure electronic evidence in an expedited manner. These may be applied with respect to any data, any crime and any physical or legal person. An order of an investigative judge is required. Additional measures are available for serious crime (Article 142-b CPC). These articles are frequently used and also applied for banks and other financial institutions. The data retention obligation offers additional possibilities to secure electronic evidence. <u>Regarding international procedures (Article 29 Budapest Convention):</u> In the absence of specific preservation provisions for domestic and international requests, the temporary seizure powers and chapter XXX on international cooperation of the current CPC may be used. Article 505 may be used to execute a request on the basis of the Budapest Convention. The Basic Public Prosecutors Office in Skopje serves as 24/7 point of contact. So far, no international preservation requests have been sent or received. Note: a new CPC enters into force on 26 November 2013. Article 184 may provide the basis for preservation orders.	<u>Article 16 Budapest Convention:</u> "The former Yugoslav Republic of Macedonia" is in line with Article 16 Budapest Convention. <u>Article 29 Budapest Convention:</u> "The former Yugoslav Republic of Macedonia" is in line with Article 29 Budapest Convention. The system has not yet been tested. The actual use of international preservation requests should be promoted.

31. Ukraine	Regarding domestic procedures (Article 16 Budapest Convention): Specific provisions on expedited preservation have not been adopted. A new CPC entered into force on 19 November 2012. "Collecting information from electronic information systems" is considered an interference in private communication (see Article 258). While Articles 262, 263, 264 and 265 may allow for access to data upon a judicial order, such powers seem to be available only for serious crime (see Article 246.2). It remains to be seen whether Article 259 (Preservation of information) may be applicable. The data retention obligation (3 years) offers additional possibilities to secure electronic evidence, but under the new CPC this may only apply to serious crime. Regarding international procedures (Article 29 Budapest Convention): The above also applies to international requests.	Article 16 Budapest Convention: Ukraine is not in line with Article 16 Budapest Convention. Further amendments to the new CPC may need to be considered Article 29 Budapest Convention: Ukraine is not in line with Article 29 Budapest Convention. Further amendments to the new CPC may need to be considered
32. United Kingdom	Regarding domestic procedures (Article 16 Budapest Convention): The UK does not have specific provisions for expedited preservation but a range of powers are used to secure electronic evidence in an expedited manner. These include s.102 of the Anti-Terrorism, Crime & Security Act (ATCS) 2001 together with a voluntary code of practice, pursuant to s.102. Law enforcement also have at their disposal the provisions of the Regulation of Investigatory Powers Act (RIPA) 2000 and Schedule 1 of the Police and Criminal Evidence Act (PACE) 1984. The procedure used will depend on the case, but a request can be made to the data owner for preservation to be done, usually by a police officer. The police may obtain a warrant from a judge to produce or provide access under the Police and Criminal Evidence Act (PACE) 1984, or a production order under Section 1 of PACE, and attend the premises where the preservation needs to be done. The police may also use RIPA, following the appropriate process for obtaining a RIPA warrant. These processes can be used for all investigations into crimes committed online. Service providers have also provided considerable assistance during emergency situations. Sharing of data on a police-to-police basis is covered by UK MLA guidance. UK data owners may provide data without MLA requests if they choose to do so. The guidelines are available at	Article 16 Budapest Convention: The UK is in line with Article 16 Budapest Convention. Article 29 Budapest Convention: The UK is in line with Article 29 Budapest Convention.

	http://www.homeoffice.gov.uk/publications/police/operational-policing/mla-guidelines?view=Binary In Scotland, common law search warrants are used. Search, seizure, access to information or production orders can be obtained expeditiously. The use of expedited preservation is considered essential in investigations and very relevant compared with other measures. The data retention obligation offers additional possibilities to secure electronic evidence. Access to retained data can be obtained expeditiously. The UK has data retention legislation, in line with the rest of the European Union, and these are set out in the Data Retention (EC Directive) Regulations 2009. Regarding international procedures (Article 29 Budapest Convention): The powers used to secure electronic evidence expeditiously at the domestic level combined with existing MLA arrangements are applied for international requests. Existing mutual legal assistance arrangements provide for executing international requests. Once the request is received and approved, the data can be obtained through legal powers and voluntary arrangements. Each request is dealt with on a case-by-case basis, and would include such considerations as dual-criminality. The Serious Organised Crime Agency (SOCA) 24/7 network point has the competence to receive and execute requests. The request needs to go to SOCA, who log the request and pass it to the appropriate law enforcement group to deal with it. Evidence is then gathered and managed as specified by the MLA provisions, as set out at http://www.homeoffice.gov.uk/publications/police/operational-policing/mla-guidelines?view=Binary	
33. United States of America	Regarding domestic procedures (Article 16 Budapest Convention): Expedited preservation is provided for in Title 18, Section 2703(f) in U.S. Federal Criminal Code. It covers any type of data in relation to any crime. A preservation request is not a judicial or prosecutorial order. Any U.S. government official, including a law enforcement agent, is authorized to issue a preservation request.	Article 16 Budapest Convention: The USA is in line with Article 16 Budapest Convention.

	Typically, when an investigation reveals that someone, such as a service provider, may hold data in an account related to the investigation, the investigator or prosecutor will send a "preservation letter" to the service provider. This letter describes the account and the types of data to be preserved. The letter may be delivered to the service provider by facsimile, email or mail. Some major providers have online request forms. Upon receipt of the government request, the service provider must take action to preserve the data related to the request. Preservation is considered a crucial and often-used tool for U.S. investigations. Several thousand requests are issue per year. The US does not have a data retention law. <u>Regarding international procedures (Article 29 Budapest Convention):</u> The legal basis for the execution of international preservation requests is the same as for domestic requests. The primary U.S. entities with competency to receive and execute international preservation requests are: ▪ Office of International Affairs, Criminal Division, U.S. Department of Justice ▪ Computer Crime and Intellectual Property Section (CCIPS), Criminal Division, U.S. Department of Justice ▪ U.S. law enforcement attachés at U.S. embassies worldwide In addition, any U.S. government official, including law enforcement agents, may issue an international preservation request. When the U.S. government acts on behalf of a foreign government, all requests for transfers of data must be made through a MLA process. Data preservation does not include the disclosure of data to the U.S. government. CCIPS processes hundreds of requests each year. Preservation is ordered usually within 24 hours of receipt of request.	<u>Article 29 Budapest Convention:</u> The USA is in line with Article 29 Budapest Convention.

3 Implementation of Articles 17 and 30 – Expedited preservation and partial disclosure of traffic data (domestic/international)

3.1 About Articles 17 and 30

3.1.1 Article 17

Article 17 complements Article 16 with specific obligations regarding the expedited disclosure of traffic data. Often, more than one service provider may be involved in the transmission of a communication. Under Article 17, service providers are to disclose sufficient data to allow identification of the path of a communication and thus that preservation orders can be served to all providers.

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.

3.1.2 About Article 30

Article 30 complements Article 29 and is the international equivalent of Article 17. Under Article 30, Parties that have been requested to preserve data under Article 29 are to disclose to the requesting Party sufficient data to allow the identification of service providers in other states that have been involved in a communication, so that additional preservation requests can be sent to these states.

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.

3.2 Implementation of Articles 17 and 29: overview

3.2.1 Domestic powers, procedures and experience (Article 17)

Specific legal provisions on expedited preservations and partial disclosure of traffic data have been put in place in:

- Albania: Article 299/b Criminal Procedure Code
- Finland: Coercive Measures Act, Chapter 4, Sections 4b
- Latvia: Specific provision of Section 191 CPC
- Moldova: Article 7f and g of the Law on Preventing and Combating cybercrime (No 20-XVI of 3 February 2009)
- Netherlands: Article 126 (2) of Dutch Code of Criminal Procedure (November ??)
- Norway: Electronic Communication Act Section 2-9 and the Criminal Procedure Act Section 118, first subsection
- Portugal: Article 13 of the Law on Cybercrime (Law nº 109/2009)
- Romania: Article 54 of Law 161/2003
- USA: U.S. Federal Criminal Code, Title 18, Section 2703(c)

Other Parties report the use of other powers – mostly production orders – to obtain the disclosure of data that would allow to identify the path of a communication and thus to serve additional preservation orders.

This is a valid approach if the procedure is expedited and not too complex. Most Parties using production orders and other powers suggest that judicial orders are needed but that these could be obtained without too much delay.

At the same time, only few countries make frequent use of this measure, namely Moldova, Norway and the USA. This means that even among Parties that have adopted specific legal provisions, it is not applied very often. In Romania, partial disclosure is part of the preservation process.

As some other Parties, Romania has adopted a specific provision in Article 54(5) of Law 161/2003. However, the difference to most other Parties is that in Romania service providers served with a preservation order are obliged automatically to disclose sufficient elements permitting to identify the path of a communication. A separate order to disclose traffic data is thus not required.

Portugal adopted a similar approach (Article 13 of Law 109/2009).

Some Parties refer to the fact that because of data retention obligations, this measure is not required. In this connection, a specific issue was raised by Estonia and Portugal that may also cause problems in other countries: in States having implemented the EU Data Retention Directive, including its purpose limitation, it may be difficult to obtain the disclosure of any traffic data unless the request is in relation to serious crime as defined under domestic law.

3.2.2 International procedures and experience (Article 30)

Only few Parties seem to make use of Article 30, namely Bulgaria, Moldova and Norway. The main reason seems to be that in most States the partial disclosure of traffic data and transmission to foreign authorities requires an MLA process and is thus not sufficiently expedited.

In some Parties, if the authorities of the requested country obtain the traffic data needed under their own investigation, they may share them with the requesting authority.

The Norwegian Internet service Opera Software is one example where traffic data may lead to third countries. Opera offers a browser for mobile data units (mobile phones etc.), Opera Mini. The browser requests web pages through Opera Software's servers, which process and compress them before sending them to the mobile data unit. This process speeds up transfer and reduces the amount of data transferred. Another result is that traffic data for Opera Mini users around the world, will pass though Opera Software's servers in Norway and other countries. Opera Mini is not a VPN or proxy service as such, but users who access the Internet via the Opera Mini browser will get a Norwegian IP address, and it's necessary to contact Opera Software to identify the end user (if possible). NCIS Norway receives international requests regarding Opera Software regularly.

3.3 Implementation of Articles 17 and 30 (partial disclosure domestic/international) – Assessment

Party	Legal provision and practical experience	Assessment
1. Albania	Regarding domestic procedures (Article 17 Budapest Convention): A specific provision on partial disclosure is available with Article 299/b CPC. The person ordered to preserve data is obliged to ensure that all data is available even if more than one service provider is involved in the transmission of a communication. The person is to disclose to the prosecutor or judicial police a sufficient amount of information to enable the identification of other service providers and the path of the communication. The measure has not been tested yet in practice. Traffic data is also retained under data retention regulations. Regarding international requests (Article 30 Budapest Convention): The procedure can also be used for international requests and was recently applied in practice.	Article 17 Budapest Convention: Albania is in line with Article 17. Article 30 Budapest Convention: Albania is in line with Article 30.
2. Armenia	Regarding domestic procedures (Article 17 Budapest Convention): No specific legal provisions are available. Search and seizure provisions of the CPC may be used or the Law on Operational Activities during the pre-investigation phase. However, there is no practical experience yet. Regarding international requests (Article 30 Budapest Convention): Not yet implemented.	Articles 17 and 30 Budapest Convention: Armenia is not in line with Articles 17 and 30. Armenia is cooperating with the Council of Europe to reform the legislation. The authorities may wish to implement Articles 17 and 30 in this context (see assessment of Article 16).

Party	Legal provision and practical experience	Assessment
3. Azerbaijan	<u>Regarding domestic procedures (Article 17 Budapest Convention):</u> No specific legal provision are available but production orders may be used under Article 10 of Law on Investigative Activities and Articles 143.2 and 445 CPC A court order is required for the production of traffic data and may take two to seven days. In addition: Administrative orders used for preservation include partial disclosure requests. This procedure may take less than one working day. No court order is needed for preservation or partial disclosure. Traffic data is also retained under bilateral agreements between the Ministry of National Security and service providers based on Article 39 of the Law on Telecommunications. <u>Regarding international requests (Article 30 Budapest Convention):</u> International requests can be processed on the basis of the Law on Mutual Legal Assistance, the Budapest Convention, other agreements and reciprocity. A request received by the 24/7 point of contact is examined and if in compliance with national security interests and obligations under international agreements is sent by the Head of General Directorate for Combating Transnational Organised Crimes to Cybercrime Unit 2 that is interacting with service providers. Once collected, the data is sent to the requesting state. No MLA procedure is required to disclose a sufficient amount of traffic data as per Article 30. This procedure is applied 4-5 times per year.	<u>Article 17 Budapest Convention:</u> Azerbaijan is in line with Article 17 although the authorities may wish to adopt specific legal provisions. <u>Article 30 Budapest Convention:</u> Azerbaijan is in line with Article 30.

4. Bosnia and Herzegovina	<u>Regarding domestic procedures (Article 17 Budapest Convention):</u> No specific legal provisions are available at State or entity levels. With regard to expedited preservation (Article 16 Budapest Convention) Art. 72a of the State CPC may be used (but also Art. 137. of CPC of RS, Art. 86a of the Federation CPC and Art. 72a of CPC of Brcko District). Under this provision, a prosecutor or police officer (with the consent of a prosecutor) sends a request to a court which issues a production order. The authorities have no practical experience regarding the partial disclosure. <u>Regarding international requests (Article 30 Budapest Convention):</u> For the powers used for preservation and disclosure court orders are required. Thus for the disclosure of preserved traffic data, an MLA procedure is needed. However, under Article 4 of the Law on Mutual Legal Assistance in Criminal Matters (BH Official Gazette, No. 53/09): "(3) In urgent cases, when such a communication is envisaged by an international treaty, requests for mutual legal assistance may be transmitted and received through the Interpol." "(6) Requests for mutual legal assistance may also be received if transmitted via electronic or some other means of telecommunication with a written record, and if the foreign relevant judicial authority is willing, upon request, to deliver a written evidence of the manner of transmission and the original request, provided that this manner of transmission is regulated in an international treaty." It is therefore possible to apply Article 30 in urgent cases, although it has not been applied yet in practice.	<u>Article 17 Budapest Convention:</u> Bosnia and Herzegovina is partially in line with Article 17. It is advisable that Bosnia and Herzegovina reform its procedural law and adopt specific provisions in line with the Budapest Convention. <u>Article 30 Budapest Convention:</u> Bosnia and Herzegovina is partially in line with Article 30.
5. Bulgaria	<u>Regarding domestic procedures (Article 17 Budapest Convention):</u> Preservation and partial disclosure orders are possible under the broad powers defined in Article 159 of the Criminal Procedure Code which obliges legal and physical persons to "preserve and hand over" computerised data, including traffic data and other objects that may be of significance to the case.	<u>Article 17 Budapest Convention:</u> Bulgaria is in line with Article 17 although the authorities may wish to adopt specific legal provisions.

	Traffic data is also retained under data retention regulations. Regarding international requests (Article 30 Budapest Convention): There are no special provisions for partial disclosure for domestic or international purposes. For international requests Bulgaria uses general provisions to obtain the full disclosure at the domestic level but discloses to foreign authorities only the partial information needed. A formal MLA request is not necessary. This approach is applied in practice.	Article 30 Budapest Convention: Bulgaria is in line with Article 30.
6. Croatia	Regarding domestic procedures (Article 17 Budapest Convention): While no specific provision on partial disclosure is available, a combination of measures may be applied such as Article 261 and 263 CPC. Art. 335 (2) CPC obliges providers to provide technical assistance to police authorities. Furthermore, Article 68 of the Police Duties and Powers Act provides broad powers to police officers to request providers to "check the identity, duration and frequency of contacts between specified telecommunication addresses". The check "may include also the determination of the place where persons establishing the telecommunications contact are situated …" Measures to obtain the partial disclosure of traffic data are not used often, but may be relevant in some investigations. Traffic data is also retained under data retention regulations implemented in the Electronic Communications Act, which follows generally provisions of the Data Retention Directive. The retention period is 12 months. Regarding international requests (Article 30 Budapest Convention): As there have until now not been any cases of requests under article 30, there is no established practice in this regard. From a normative perspective, it should be noted that a 24/7 point of contact, required by the Convention, has been established at the Department for Economic Crime and Corruption, General Police Directorate. This	Article 17 Budapest Convention: Croatia is in line with Article 17 although the authorities may wish to adopt specific legal provisions. Article 30 Budapest Convention: Croatia is in line with Article 30 although the authorities may wish to adopt specific legal provisions, and promote the use of the provision in practice.

	contact point is able to follow up on the request under art. 30 of the Convention and obtain necessary information (data necessary to identify that service provider and the path of the communication) through so called Operational-Technical Centre (state body authorized to perform surveillance of communications, which has direct access to service providers). In general, the Act on Cooperation in Criminal Matters would allow that the point of contact provides information requested under article 30 without a formal MLA request which case it would also be possible to provide it expediently (less than 24 hours).	
7. Cyprus	Regarding domestic procedures (Article 17 Budapest Convention): As explained in relation to Article 16, all service providers are obliged to retain all traffic data, location data and the related data necessary to identify the subscriber or user for a period of six months. The procedure to secure a judicial warrant for such data, based on Law 183(I)/2007, according to practice, is relatively expeditious. An application is prepared by the police and after it is checked and approved by the Attorney General's Office - within the same day- an ex parte (without notifying the service provider) application is filed at the Court. A decision for granting or refusing the warrant is usually issued the same day. However, the limitations regarding serious crime apply. Regarding international requests (Article 30 Budapest Convention): The disclosure of traffic data is only possible under the provisions of Law 183(I)/2007 and subject to the conditions and safeguards provided there. The expedited disclosure of a sufficient amount of traffic data to determine the path of a communication would therefore not be possible or only in limited circumstances.	Article 17 Budapest Convention: Cyprus is partially in line with Article 17 Budapest Convention. The authorities may wish to adopt specific legal provisions. Article 30 Budapest Convention: Cyprus is not in line with Article 30 Budapest Convention. The authorities may wish to adopt specific legal provisions.
8. Denmark	[Denmark did not reply to the questionnaire]	Article 17 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision.

		Article 30 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision.
9. Estonia	Regarding domestic procedures (Article 17 Budapest Convention): Estonia has not adopted specific provisions on expedited preservation and partial disclosure. However, the general powers of § 215 CPC may be used that obliges anybody to comply with orders and demands of investigative bodies and prosecutors' offices. In most cases, direct search, seizure and production orders rather than provisional measures are applied in line with principles of necessity and proportionality. Traffic and subscriber data is retained by providers under the Electronic Communications Act (§ 111 – 113). Disclosure of traffic data is permitted only with regard to serious criminal offences (sanction must be at least 3 years imprisonment). This suggests that the partial disclosure of traffic data (also through seizure, production orders or general powers) is not possible for all crimes. Regarding international requests (Article 30 Budapest Convention): For this measure, an official MLA request is necessary and principles of judicial cooperation apply. The measure has not been used in practice. In cases of urgency, a request submitted through the International Criminal Police Organisation (Interpol) or a notice in the Schengen Information System may be complied with the consent of the Public Prosecutor's Office before the request for legal assistance is received by the Ministry of Justice.	Article 17 Budapest Convention: Estonia is partially in line with Article 17 Budapest Convention. The measure is currently only possible with regard to serious crime. New legislation is to enter into force on 1 January 2013 which will allow access to retained data to a broader range of offences. According to the amendments to the Criminal Procedure Code, preservation and disclosure of data (including traffic data) is allowed with regard to any criminal offence. Article 30 Budapest Convention: Estonia is partially in line with Article 30 Budapest Convention. The measure has not been applied yet. The fact that formal MLA procedures would apply suggests that expedited disclosure to a requesting party is difficult. However, in urgent cases expedited disclosure would be possible.
10. Finland	Regarding domestic procedures (Article 17 Budapest Convention): Finland adopted a specific provision on expedited preservation and partial disclosure in Chapter 4, Section 4b an 4c of the Coercive Measures Act (450/1987) as amended in 2007 (this corresponds to Chapter 8, Sections 24-26 in the reformed Coercive	Article 17 Budapest Convention: Finland is in line with Article 17 Budapest Convention.

	Measures Act (806/2011). In practice, however, seizure provisions are used to obtain data with respect to domestic investigations. <u>Regarding international requests (Article 30 Budapest Convention):</u> The above measure can also be applied for international requests. General grounds for refusal to provide assistance are listed in Sections 12 and 13 of the Act on International Legal Assistance in Criminal Matters (4/1994) (prejudice to sovereignty, security, essential interests; contrary to principles of human right or ordre public; political offence and similar). Act (4/1994) is a general MLA law which can be applied also in relations with non-contracting parties. Therefore it is worth noting that this general MLA law also has a provision (§ 30) which states that regardless the provisions of this law Finland provides assistance as specifically agreed e.g. in international Conventions.	<u>Article 30 Budapest Convention:</u> Finland is in line with Article 30 Budapest Convention, although the provision has not yet been tested in practice.
11. France	<u>Regarding domestic procedures (Article 17 Budapest Convention):</u> France has not adopted specific provisions on partial disclosure. Seizure and other powers may be used. Orders to providers may cover not only requests for preservation but also partial disclosure. Traffic data is furthermore retained under data retention regulations. <u>Regarding international requests (Article 30 Budapest Convention):</u> The same approach is used for international requests: A service provider executing a preservation request informs LEA as to whether a server under investigation is managed from an IP address in a 3rd country. French LEA will then inform the requesting LEA accordingly. The measure is rarely used.	<u>Article 17 Budapest Convention:</u> France is in line with Article 17. While a specific regime for the partial disclosure is not available, seizure and other powers may be applied in an expedited manner. <u>Article 30 Budapest Convention:</u> France is in line with Article 30.

12. Georgia	Regarding domestic procedures (Article 17 Budapest Convention): Specific provisions on partial disclosure have not been adopted, but other powers are used, in particular Article 136 CPC on production orders. Production orders are used frequently as shown in an analysis of 17 judgements in 2011 and 2012 which include requests to service providers to provide data on the relevant IP history, and similar. The analysis shows a response time by providers within three days. Regarding international requests (Article 30 Budapest Convention): As partial disclosure is possible under the domestic procedure (under Article 136 CPC), Georgia seems to be able to cooperate internationally through the newly created Specialised Cybercrime Unit of Central Criminal Police Department that has the responsibilities of a 24/7 point of contact, including international cooperation. It may therefore be possible to cooperate in cases related to Article 30 Budapest Convention but this has not yet been tested in practice.	Article 17 Budapest Convention: Georgia is partially in line with Article 17 Budapest Convention. The adoption of specific legal provisions may be considered. Article 30 Budapest Convention: Georgia is partially in line with Article 30 Budapest Convention.
13. Germany	Regarding domestic procedures (Article 17 Budapest Convention): In the absence of a specific provision on partial disclosure, the approach used with respect to Article 16 may also be used with respect to Article 17. However, limitations apply with respect to traffic data in relation to offences that are not confirmed to be serious in nature and with respect to offences not committed by means of computer systems. Regarding international requests (Article 30 Budapest Convention): At the domestic level, traffic data may be obtained using the procedures described in relation to Article 16 and 29. A request under Article 29 and containing sufficient information (see Article 29.2) is considered a sufficiently formal MLA request. If such a request under Article 29 comprises also the partial disclosure of traffic data, such data can be disclosed.	Article 17 Budapest Convention: Germany is partially in line with Article 17 Budapest Convention. Some limitations regarding the disclosure of traffic data apply. The adoption of specific legal provisions may be considered. The comments regarding Articles 16 and 29 Budapest Convention apply as well. Article 30 Budapest Convention: Germany is partially in line with Article 30 Budapest Convention. A sufficient amount of traffic data can be disclosed to foreign authorities but limitations apply. The comments regarding

	However, the above limitations regarding traffic data apply. Moreover, under the Law on International Judicial Cooperation in Criminal Matters (Sec. 61 and 92 IRG) that allows for providing spontaneous information with a formal MLA request.	Articles 16 and 29 Budapest Convention apply as well.
14. Hungary	<u>Regarding domestic procedures (Article 17 Budapest Convention):</u> Specific provisions on partial disclosure have not been adopted, but seizure orders may be used to obtain traffic data. <u>Regarding international requests (Article 30 Budapest Convention):</u> Specific provisions are not available, and alternative means to obtain and disclose partial traffic data to foreign authorities have not been tested in practice. It seems that a formal mutual legal assistance request would be required and a domestic investigation would need to be opened.	<u>Article 17 Budapest Convention:</u> Hungary is partially in line with Article 17 Budapest Convention. <u>Article 30 Budapest Convention:</u> Hungary is not in line with Article 30 Budapest Convention. The partial disclosure of traffic data appears not be feasible without a formal mutual legal assistance request and a domestic investigation.
15. Iceland	[Iceland did not reply to the questionnaire]	<u>Article 17 Budapest Convention:</u> The T-CY has not been able to determine whether the Party is in line with this provision. <u>Article 30 Budapest Convention:</u> The T-CY has not been able to determine whether the Party is in line with this provision.

16. Italy	Regarding domestic procedures (Article 17 Budapest Convention): Article 132, paragraphs 1,1a and 3 of the Data Protection Act may be used for requests to produced traffic data: As part of the investigation activities, the judicial police generally asks the prosecutor to issue a decree to acquire the traffic data needed to ascertain the offence and to identify the author; the Public Prosecutor, after having established that the conditions of law are met, issues a decree under art. 256 CPC; the notification of the action against the Internet Service Provider (ISP) or other provider of public electronic communication is made by the Judicial Police empowered by the judicial authority; the data requested are delivered to the judicial police who transmits them to the delegating judicial authority. Regarding international requests (Article 30 Budapest Convention): The above procedure can also be applied in cases of international requests.	Article 17 Budapest Convention: Italy is in line with Article 17 Budapest Convention. Article 30 Budapest Convention: Italy is in line with Article 30 Budapest Convention.
17. Latvia	Regarding domestic procedures (Article 17 Budapest Convention): Latvia adopted a specific provision on partial disclosure in Section 192 CPC. A decision by an investigating judge or consent by the data subject is required. In practice, this measure is not considered relevant at the domestic level since service providers store data under data retention regulations. Regarding international requests (Article 30 Budapest Convention): Section 192 CPC can also be applied to international requests. The practical procedure is similar to an international preservation request under Article 29 Budapest Convention. If in the course of a preservation request, it becomes know that a service provider in a third state was involved in the transmission of a communication, the Cybercrime Combating and IPR Protection Unit notifies the 24/7 point of contact of Latvia who notifies the requesting Party without delay. Latvia has received and executed requests of this nature. Latvia has sent similar requests abroad but the other Party hasn't disclosed the data.	Article 17 Budapest Convention: Latvia is in line with Article 17 Budapest Convention. Article 30 Budapest Convention: Latvia is in line with Article 30 Budapest Convention.

18. Lithuania	Regarding domestic procedures (Article 17 Budapest Convention): Lithuania has not adopted specific provisions on partial disclosure. The general powers to obtain / obligation to provide information can be applied (Article 155 CPC). Depending on the specific situation Article 65 Paragraph 2 of the LEC, Article 18 Paragraph 1 Subparagraph 11 of the Law on Police Activities, Articles 147, 155, 205 or 207 of the CPC could be applied to obtain the partial disclosure of traffic data. However, these possibilities have not yet been tested in practice to. As traffic data is also retained under data retention obligations, the partial disclosure is not considered essential for domestic investigations. Agreements have been signed with large ISPs, and thus data could be obtained in an expedited manner if necessary. Regarding international requests (Article 30 Budapest Convention): So far, Lithuania not neither sent nor received international requests. MLA requests would be required for partial disclosure. However, the Lithuanian police 24/7 contact point can apply provisions of Article 18 Paragraph 1 Subparagraph 11 of the Law on Police Activities and Article 30 and 35 of the Budapest Convention, with reference to Article 3 Paragraph 4 of the Law of the Republic of Lithuania on Ratification of the Budapest Convention (No.IX-1974, January 22, 2004, entered in force since March 7, 2004; Official Gazette, No. 36-1178, 2004).	Article 17 Budapest Convention: Lithuania is partially in line with Article 17 Budapest Convention. The adoption of specific provisions may be considered. (The T-CY was informed that amendments are underway.) Article 30 Budapest Convention: Lithuania is partially line with Article 30 Budapest Convention.
19. Republic of Moldova	Regarding domestic procedures (Article 17 Budapest Convention): At the national level partial disclosure is provided by article 7 (2) which foresees for the service provider the obligation to provide the authorities with the necessary information about the chain of communication. Regarding international requests (Article 30 Budapest Convention): The above provision also applies with respect to international requests.	Article 17 Budapest Convention: Moldova is in line with Article 17 Budapest Convention. Article 30 Budapest Convention: Moldova is in line with Article 30 Budapest Convention.

20. Montenegro	Regarding domestic procedures (Article 17 Budapest Convention): Montenegro does not have a specific provision on partial disclosure but search and seizure (Article 75 CPC) and the provisional/temporary seizure (Article 85 CPC which includes electronic data) may be used as in the case of preservation requests. Judicial orders are required and they would need to specific what additional information is to be provided to other service providers and the path of a communication. However, these possibilities have not yet been tested in practice, as traffic data is also retained under data retention obligations. Regarding international requests (Article 30 Budapest Convention): So far, Montenegro not neither sent nor received international requests.	Article 17 Budapest Convention: Montenegro is partially in line with Article 17 Budapest Convention. The system is yet to be tested in practice. Specific provisions are recommended. Article 30 Budapest Convention: Montenegro is partially in line with Article 30, but the system is yet to be applied in practice.
21. Netherlands	Regarding domestic procedures (Article 17 Budapest Convention): The Netherlands have adopted a specific provision in Article 126ni (paragraph 2) of the CPC. The DCCP enables the public prosecutor, in cases of crimes for which pre-trial detention is allowed (these include almost all cybercrimes) and which seriously infringe the rule of law, to order someone to preserve data stored in a computer that are particularly vulnerable to loss or change. If the data relate to communications, the communications provider is also required to provide the data necessary for retrieving the identity of other providers whose networks or services were used in the relevant communication. Regarding international requests (Article 30 Budapest Convention): The measure can be used expeditiously through police to police cooperation.	Article 17 Budapest Convention: The Netherlands is in line with Article 17 Budapest Convention. Article 30 Budapest Convention: The Netherlands is in line with Article 17 Budapest Convention.

22. Norway	Regarding domestic procedures (Article 17 Budapest Convention): The Electronic Communication Act Section 2-9 and the Criminal Procedure Act Section 118, first subsection are used to obtain partial disclosure. Partial disclosure is important, and is used frequently by the police in Norway. The Norwegian Telecom Act Section 2-9, third section, is the legal provision for asking telecom providers for customer information. Regarding other telecom data, the Post and Telecommunications Authority must accept the request for data. The legal framework will be changed when the Data Retention Directive is implemented. The courts will decide requests for other data than customer information. The usual response time by providers is 24 hours. Regarding international requests (Article 30 Budapest Convention): Article 30 is considered relevant and used frequently. It addresses a relevant problem regarding electronic evidence and international cooperation. Increased use of VPN and proxy services is a growing challenge, because relevant data must be identified and collected in several locations and often in several jurisdictions.	Article 17 Budapest Convention: Norway is in line with Article 17 Budapest Convention. Article 30 Budapest Convention: Norway is in line with Article 30 Budapest Convention.
23. Portugal	Regarding domestic procedures (Article 17 Budapest Convention): Portugal has adopted a specific provision in Art. 13 Law on Cybercrime (Law 109/2009). A letter from a prosecutor or in urgent cases from a police officer is sufficient. As traffic data is also retained under the Data Retention Law and access requires a court order and is limited to serious crime. ISPs are therefore less cooperative in the disclosing traffic data. Regarding international requests (Article 30 Budapest Convention): Portugal has adopted a specific provision for international requests for partial disclosure (Article 22 of Law 109/2009). Under 22.10, traffic data identifying other service providers in the path of a communication will be quickly communicated to the	Article 17 Budapest Convention: Portugal is in line with Article 17 Budapest Convention. Article 30 Budapest Convention: Portugal is in line with Article 30 Budapest Convention.

	requesting foreign authority.	
24. Romania	<u>Regarding domestic procedures (Article 17 Budapest Convention):</u> Romania has adopted a specific provision in Article 54 of Law 161/2003. Under Article 54(5), service providers served with a preservation order are obliged automatically to disclose sufficient elements permitting to identify the path of a communication. A separate order to disclose traffic data is thus not required. In practice, service providers use partial disclosure to inform the prosecutor if they are not in a position to carry out a preservation order by different reasons (termination of service, new agreements etc.). As traffic data is also retained under data retention obligations. <u>Regarding international requests (Article 30 Budapest Convention):</u> Romania has adopted a specific provision for international requests in Article 64 of Law 161/2003. The prosecutor of the Service for Combating Cybercrime can immediately share partially disclosed traffic data with the requesting foreign authority.	<u>Article 17 Budapest Convention:</u> Romania is in line with Article 17 Budapest Convention. <u>Article 30 Budapest Convention:</u> Romania is in line with Article 30 Budapest Convention.
25. Serbia	<u>Regarding domestic procedures (Article 17 Budapest Convention):</u> Serbia has not adopted a specific provision on partial disclosure but different powers can be used: Criminal Code article 112, Law on Public Prosecution article 5, existing Criminal Procedural Code articles 46, 49, 77, 78, 82, 85, 225, 234, 235, 504e, 504ž, 504lj (new CPC implementation from 2013), Law on the organization and competence of government authorities for combating cybercrime 2, 3, 4, 5 and 6, Law on Electronic Communications articles 126, 127, 128, 129 and 130, Rules on general terms and conditions for performing EC activities under the general authorization regime 31, 34. The measure may be relevant in early pre-criminal investigations. When needed LEA, Prosecutor or Court depending on the phase of the criminal proceedings issues a request or order in accordance with the Law. Traffic data is also retained under data retention obligations.	<u>Article 17 Budapest Convention:</u> Serbia is in line with Article 17 Budapest Convention although specific provisions should be considered. <u>Article 30 Budapest Convention:</u> Serbia is in line with Article 30, although specific provisions should be considered.

	Regarding international requests (Article 30 Budapest Convention): The powers for domestic investigations can also be used in connection with international mutual legal assistance requests. However, they are rarely applied as the MLA procedure is considered too complex.	
26. Slovakia	Regarding domestic procedures (Article 17 Budapest Convention): Section 90 CPC covers the preservation and disclosure of computer data and would thus also cover the partial disclosure of traffic data in line with Article 17 Budapest Convention. It is unclear however, whether recent amendments to the CPC (Act. No. 262/2011) still allow for partial disclosure. Regarding international requests (Article 30 Budapest Convention): [no information received]	Article 17 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision. Article 30 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision.
27. Slovenia	Regarding domestic procedures (Article 17 Budapest Convention): Slovenia has not adopted a specific provision on partial disclosure but the procedures referred to in relation to Article 16 can also be applied for Article 17. In practice, such powers are rarely used to obtain the partial disclosure. Traffic data is also retained under data retention obligations. Regarding international requests (Article 30 Budapest Convention): The procedures referred to in relation to Article 29 may also be applied for Article 30. Article 515 CPC allows a police/prosecutor/judge to provide direct assistance to foreign law enforcement agencies by using e-mail or similar means. This Article in the Slovenian CPC can be used for the partial disclosure of computer data to other Parties in line with Article 30 Budapest Convention.	Article 17 Budapest Convention: Slovenia is partially line with Article 17 Budapest Convention, although the system is yet to be tested in practice. Slovenia may want to consider introducing specific legal provisions. Article 30 Budapest Convention: Slovenia is partially in line with Article 30 but the system is yet to be tested in practice. Slovenia may want to consider introducing specific legal provisions.

28. Spain	Regarding domestic procedures (Article 17 Budapest Convention): According to the replies received, Spain has adopted data retention regulations in line with the EU Directive covering traffic data and subscriber information and pertaining to service providers. Specific provisions on partial disclosure have not been adopted. Regarding international requests (Article 30 Budapest Convention): A mutual legal assistance request would be required for partial disclosure and disclosure would only be possible for serious crime.	Article 17 Budapest Convention: Spain is not in line with Article 17 Budapest Convention. Disclosure of traffic data is only possible for serious crime. Spain may want to consider introducing specific legal provisions. Article 30 Budapest Convention: Spain is not in line with Article 30
29. Switzerland	Regarding domestic procedures (Article 17 Budapest Convention): Switzerland has not adopted specific provisions in this respect. Article 273 CCP enables prosecuting authorities to ask for the disclosure of traffic, invoice and subscriber data when there is the suspicion that a crime or offence has been committed. The order requires the approval through a court. The possibility is not restricted to a certain number or range of crimes, but is generally applicable and can also be employed retrospectively. In addition to that, article 14 paragraph 4 of the Law on Surveillance is applicable, stating that an ISP is obliged to deliver all the necessary data to enable the authorities to investigate the author of an offence committed by means of the Internet. Taking into account that this is not considered to be a measure of surveillance in a narrow sense, the request can be made in a direct manner, not depending on the gravity of the offence. The public prosecutor requests, if the requirements according to article 273 CCP are met, information with regard to traffic, invoice or subscriber data. The prosecutor submits, within 24 hours from the release of the information, the necessary documents for authorization by the compulsory measures court. The court shall decide within 5 days from the release of the information being ordered (art. 274 CCP). Regarding international requests (Article 30 Budapest Convention): Insufficient information available	Article 17 Budapest Convention: Switzerland is in line with Article 17 Budapest Convention Article 30 Budapest Convention: The T-CY has not been able to determine whether the Party is in line with this provision.

30. "The former Yugoslav Republic of Macedonia"	Regarding domestic procedures (Article 17 Budapest Convention): Specific provisions on partial disclosure have not been adopted. However, seizure provisions of Article 203 of CPC may be used, as well as Article 142b (special investigative means for serious crime including search and seizure of computer systems or databases). An order from an investigative judge is needed. The system has not yet tested in practice. The new CPC that enters into force on 26 November 2013 also contains no specific provisions, but Article 184 on the search of computer systems and data may be used. Regarding international requests (Article 30 Budapest Convention): The above provisions may also be applied for international requests. Note: It remains to be seen how measures under Articles 17 and 30 can be applied under the new Criminal Procedure Code as of 26 November 2013.	Article 17 Budapest Convention: "The former Yugoslav Republic of Macedonia" is partially in line with Article 17 Budapest Convention. The system is yet to be tested in practice. Specific provisions should be considered. Article 30 Budapest Convention: "The former Yugoslav Republic of Macedonia" is partially in line with Article 30 Budapest Convention.
31. Ukraine	Regarding domestic procedures (Article 17 Budapest Convention): Specific provisions on partial disclosure have not been adopted. A new CPC entered into force on 19 November 2012. Under this CPC, a partial disclosure would be considered interference in private communications that is only possible by court order and for serious crime. The specific cybercrimes of the Ukrainian Criminal Code (articles 361 – 363-1) are not considered serious crime, and thus partial disclosure would not be possible unless they are linked to other, serious crimes. Regarding international requests (Article 30 Budapest Convention): A mutual legal assistance request would be required to disclose traffic data, but the above restrictions would apply.	Article 17 Budapest Convention: Ukraine is not in line with Article 17. Ukraine may wish to consider amendments to the CPC. Article 30 Budapest Convention: Ukraine is not in line with Article 30.

32. United Kingdom	Regarding domestic procedures (Article 17 Budapest Convention): The UK does not have specific provisions for partial disclosure. A number of powers can be used – as in the case of expedited preservation – such as the data retention regulations 2009 and the Acquisition and Disclosure of Communications Data: Code of Practice pursuant to section 71 of the Regulation of Investigatory Powers Act 2000 in order to determine the path of a communication. Access to retained data can be obtained expeditiously through a variety of provisions. These include s.102 of the Anti-Terrorism, Crime & Security Act (ATCS) 2001 together with a voluntary code of practice, pursuant to s.102. Law enforcement also has at their disposal the provisions of the Regulation of Investigatory Powers Act (RIPA) 2000 and Schedule 1 of the Police and Criminal Evidence Act (PACE) 1984. The procedure used will depend on the case, but a request can be made to the data owner for preservation to be done, usually by a police officer. The police may obtain a warrant from a judge to produce or provide access under the Police and Criminal Evidence Act (PACE) 1984, or a production order under Section 1 of PACE, and attend the premises where the preservation needs to be done. The police may also use RIPA, following the appropriate process for obtaining a RIPA warrant. These processes can be used for all investigations into crimes committed online. Service providers have also provided considerable assistance during emergency situations. Sharing of data on a police-to-police basis is covered by UK MLA guidance. This set out in: http://www.homeoffice.gov.uk/publications/police/operational-policing/mla-guidelines?view=Binary In Scotland common law searches are used. Regarding international requests (Article 30 Budapest Convention): As for Art 17, the powers used to secure electronic evidence expeditiously at the domestic level combined with existing MLA arrangements are applied for international requests. Existing mutual legal assistance arrangements provide for executing international requests. Once the request is received and approved, the data can be obtained through legal powers and voluntary arrangements. Each request is dealt with	Article 17 Budapest Convention: The UK is in line with Article 17 Budapest Convention. Article 30 Budapest Convention: The UK is in line with Article 30 Budapest Convention. Information can be provided through police to police cooperation.

	on a case-by-case basis, and would include such considerations as dual-criminality. The Serious Organised Crime Agency (SOCA) 24/7 network point has the competence to receive and execute requests. The request needs to go to SOCA, who log the request and pass it to the appropriate law enforcement group to deal with it. Evidence is then gathered and managed as specified by the MLA provisions. These processes can be used for all investigations into crimes committed online. Service providers have also provided considerable assistance during emergency situations. Sharing of data on a police-to-police basis is covered by UK MLA guidance. UK data owners may also provide data without MLA requests if they choose to do so. This is set out at: http://www.homeoffice.gov.uk/publications/police/operational-policing/mla-guidelines?view=Binary Partial disclosure is thus possible through police-to-police cooperation. The UK can provide data obtained under Art 17 to other states either under MLA arrangements or under police-to-police transfer, as set out in the UK guidelines, depending on the requirements of the requesting state.	
33. United States of America	Regarding domestic procedures (Article 17 Budapest Convention): Law enforcement officials obtain partial disclosure of traffic data by issuing a subpoena, as set forth at U.S. Code, Title 18, Section 2703(c), or a production order, Section 2703(d). When an investigation reveals that a service provider may hold data related to the investigation, the investigator may request that the prosecutor issue a subpoena or procure a production order for partial disclosure of traffic date (and other subscriber information). Subpoenas and orders for partial disclosure of traffic data and subscriber information issued by federal entities are estimated to be in the thousands each year. Regarding international requests (Article 30 Budapest Convention): The partial disclosure of traffic data and subscriber information (including data needed to identify the path of a communication in the sense of Article 30 Budapest Convention) can be carried out by MLA request. However, if the upstream provider is	Article 17 Budapest Convention: The US is in line with Article 17 Budapest Convention. Article 30 Budapest Convention: The US is partially in line with Article 30 Budapest Convention. The partial disclosure and transmission of traffic data to requesting foreign authorities requires an MLA process for upstream providers based in the US.

	not in the US, US LEA will disclose the country and the provider to the foreign requesting LEA. In addition, if US LEA independently – such as by opening their own investigation – determine that an IP address or domain name is not US-based, that information can be disclosed to the foreign requester. The provision is not much used in practice.	

4 Data preservation versus data retention

4.1 About data retention versus preservation

Some of the replies to the T-CY questionnaire and interaction with stakeholders in European and non-European States point at misperceptions regarding the concept of data preservation on the one hand and the concept of data retention on the other.

4.1.1 Expedited preservation

Articles 16 and 30 of the Budapest Convention on Cybercrime require that Parties adopt measures to enable the expedited preservation of specified computer data at domestic and international levels.

This means that law enforcement must be able to order a service provider or any other physical or legal person to preserve any specified data (traffic data, subscriber information or content data) that may be needed as evidence in a specific investigation. It refers to stored data, that is, data that already exists and not future data for which other measures (real time collection of traffic data or interception of content data) are to be applied.

Expedited preservation measures are not limited to serious crime or the offences against or by means of computers foreseen in Articles 2 – 10 of the Budapest Convention. Preservation must be possible for electronic evidence in relation to any criminal offences (Article 14.2 Budapest Convention).

It is a provisional measure, and it must be possible in a first step to order the preservation of volatile data without delay.[9] The preservation will then allow for the time needed for the second step, that is, to actually obtain the data through formal procedures, such as search and seizure or production orders which in most countries require a court order.

This provisional measure of data preservation is particularly important with respect to international cooperation, since search, seizure or production orders will most often need to await the receipt of a formal request for mutual legal assistance from the foreign requesting State.

The Budapest Convention on Cybercrime does not cover the concept of data retention.

4.1.2 Data retention

Many Parties have enacted data retention regulations, in particular following the Data Retention Directive of the European Union of 2006.[10] Governments of many other countries worldwide have also adopted or are considering data retention obligations.[11]

---

[9] Expedited preservation is also called "quick freeze" by some, although this term is misleading.

[10] "Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC". For the text see:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML
For national execution measures by EU member states to implement the Directive see:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:72006L0024:EN:NOT#FIELD_BE
Following an evaluation in 2011, the Directive is currently under review. For the evaluation report see:
http://ec.europa.eu/commission_2010-2014/malmstrom/pdf/archives_2011/com2011_225_data_retention_evaluation_en.pdf

Party	Data retention regulations
1. Albania	Yes, 2 years
2. Armenia	No
3. Azerbaijan	No (under consideration)
4. Bosnia and Herzegovina	Yes, 1 year
5. Bulgaria	Yes, 1 year. Data accessed may be retained a further 6 months
6. Croatia	Yes, 1 year
7. Cyprus	Yes, 6 months
8. Denmark	Yes, 1 year
9. Estonia	Yes, 1 year
10. Finland	Yes, 1 year
11. France	Yes, 1 year
12. Germany	No (law annulled)
13. Hungary	Yes, 6 months for unsuccessful calls, 1 year for other data
14. Iceland	Yes
15. Italy	Yes, 29 months for telephony data, 6 months for Internet data
16. Latvia	Yes, 18 months
17. Lithuania	Yes, 6 months
18. Republic of Moldova	Yes, 3 months
19. Montenegro	Yes
20. Netherlands	Yes, 1 year
21. Norway	No (entry into force pending)
22. Portugal	Yes, 1 year
23. Romania	Yes, 6 months
24. Serbia	Yes, 12 months
25. Slovakia	Yes, 1 year fixed and mobile telephony data, 6 months for Internet access, email and telephony data
26. Slovenia	Yes, 14 months telephony data, 8 months Internet-related data
27. Spain	Yes, 1 year
28. Switzerland	Yes, 6 months
29. "The former Yugoslav Republic of Macedonia"	Yes
30. Ukraine	Yes, 3 years
31. United Kingdom	Yes, 1 year
32. United States of America	No

Under the Directive, all traffic data, location data and subscriber information related to fixed network telephony and mobile telephony as well as Internet access, Internet e-mail and Internet telephony are to be retained for "periods of not less than six months and not more than two years from the date of the communication" (Article 6).

It does not cover content data, nor URLs, nor destination IP addresses, nor email headers: "It shall not apply to the content of electronic communications, including information consulted using an electronic communications network" (Article 3).

[11] Many have taken guidance from EU Data Retention Directive. It can be assumed that the results of the current review of this Directive will again provide guidance to third countries.

It should furthermore be noted that the definitions of "traffic data" and of "service providers" are more restrictive in the EU Directive than in the Budapest Convention.[12]

The Directive is to ensure that "the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law" (Article 2).[13]

The data are to be retained "to the extent that those data are generated or processed by providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned" (Article 3).

Article 7 stipulates that "(d) the data, except those that have been accessed and preserved, shall be destroyed at the end of the period of retention".[14]

The data are to be retained at the level of the service provider. The Directive leaves it to national authorities to define conditions under which criminal justice authorities can obtain access to data retained.

4.1.3 Expedited preservation versus data retention

Expedited preservation and data retention are different concepts.

Replies to the questionnaires suggest that the two are considered complementary measures that can be use applied in parallel or in combination or separately for different purposes. For example:

- A data retention obligation enhances the chances that historical traffic, location and subscriber data that are to be preserved are still available
- If the automatic retention period is about to expire, a preservation order would allow to safeguard specified data in a specific investigation beyond this period
- Retained data may only be accessed in relation to serious crime, while preservation orders may be issued and electronic evidence subsequently be obtained in relation to any crime. It has been underlined that in case of cybercrime it may not be known at the early stages of an investigation whether or not this is a case of serious crime[15]

---

[12] The Data Retention Directive applies to "providers of publicly available electronic communications services or of a public communications network within their jurisdiction in the process of supplying the communications services concerned", while the Budapest Convention in Article 1.c covers "any public or private entity that provides to users of its service the ability to communicate by means of a computer systems". The Data Retention Directive lists categories of traffic and location data to be retained, while the Budapest Convention in Article 1.d contains a more open definition of traffic data.

[13] The "purpose limitation" to serious crime has been transposed by EU member states in different ways. In some EU member states, access to retained data is possible with respect to a broader range of offences (such as in Belgium, Denmark, France, Italy, Latvia, Poland, Slovakia or Slovenia). Constitutional court rulings in Romania (October 2009), Germany (March 2010) and the Czech Republic (March 2011) annulling domestic legislation transposing the Directive underlined the need for stricter limitations and safeguards (see Evaluation report on the Data Retention Directive (COM(2011)225 final), page 20 (http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf)

[14] It seems that many non-European states have enacted data retention obligations with minimum retention periods but without the requirement to delete data at a certain point in time.

[15] An investigation of an apparently minor fraud case may reveal that an IP address is linked to a major transnational criminal operation.

- While data retention obligations refer to providers of "publicly available electronic communications services or of a public communications network within their jurisdiction", preservation orders may be issued to any legal or physical person holding data
- Article 29 and 30 Budapest Convention allow for international preservation requests also to countries without data retention obligation.

	Expedited preservation	**Data retention (Directive)**
Aim	Provisional measure to preserve volatile electronic evidence to allow for time for formal measures to obtain evidence	Ensure that data is available for investigation, detection and prosecution of serious crime
Specified/ automated	Specific order for specified data	Automatic retention of data
Type of data	Any data (including content data)	Traffic and location data and subscriber information (not content data, nor destination IP addresses, URLs, email headers, or list of cc recipients)
Purpose limitation	Any crime involving electronic evidence	Serious crime
Addressee	Any physical or legal person (not limited to service providers)	Service providers
Time period	Flexible: 90 days (renewable)	Specific retention period (6 to 24 months - to be specified in domestic law)

Most respondents, therefore, considered that both measures were necessary.

At the domestic level, data retention reduces the need for preservation orders since criminal justice authorities are able to obtain retained traffic, location or subscriber data through search, seizure or production orders without the need for provisional measures.

In fact, information available suggests that for traffic, location and subscriber data access to retained data is sought much more often than preservation orders are issued. The ratio may well be higher than 1000 requests for retained data for each 1 preservation request.[16]

The replies also suggest that the preservation measure is largely underused.

In sum, data retention complements but is not a substitute for expedited preservation. While data retention appears to be an effective tool to secure traffic, location and subscriber data, a Party having implemented data retention only, would not be fully in line with Articles 16, 17, 29, 30 of the Budapest Convention.

[16] See statistics in the Evaluation report on the Data Retention Directive (COM(2011)225 final): in 2008, the Czech Republic requested retained data 131,560 times, Denmark 3,599 times, Germany 12,684 times, Ireland 14,095 times, Spain 53,578 times, France 503,437 times, Latvia 16,892 times, Lithuania 85,315 times, Malta 869 times, Netherlands 85,000, United Kingdom 470,222 times. As indicated, several EU member states do not limit access to retained data to serious crime. These figures need to be considered with caution as they comprise access to different types of data under different rules.

5 Conclusions

The T-CY at its 7th Plenary Session (June 2012) discussed and at its 8th Plenary Session (December 2012)[17] adopted the present report assessing the implementation by the Parties of four articles of the Budapest Convention on Cybercrime:

- Article 16 – Expedited preservation of stored computer data (domestic level)
- Article 17 – Expedited preservation and partial disclosure of traffic data (domestic level)
- Article 29 – Expedited preservation of stored computer data (international level)
- Article 30 – Expedited disclosure of preserved traffic data (international level).

5.1 Conclusions and recommendations

The T-CY,

- considers that the assessment of the implementation of specific provisions of the Budapest Convention will enhance the effectiveness of this treaty;
- welcomes the replies to the T-CY questionnaire received from and the cooperation in the assessment by 31 State Parties;
- regrets that no replies have been received from Denmark and Iceland;
- calls on all Parties to actively participate in future assessments in the interest of the effectiveness of the Budapest Convention and of efficient international cooperation against cybercrime.

The T-CY adopts the following general conclusions and recommendations:

1. The expedited preservation provisions of the Budapest Convention, in particular articles 16 and 29, are highly relevant tools to secure volatile evidence in an international context. The expedited preservation of electronic evidence will allow for the time needed for formal mutual legal assistance requests.

2. A number of Parties have adopted specific legal provisions in line with Articles 16, 17, 29 and 30.

3. A considerable number of Parties refer to general powers, or search or seizure or production orders, often in combination with data retention, to preserve electronic evidence in an expedited manner. Some Parties, in this way, seem to be able to meet most of the requirements of Articles 16, 17, 29 and 30.

4. However, such powers may not represent full substitutes for preservation, particularly as to international requests. Search, seizure or production orders may be slower and harder to obtain as they require stricter safeguards and conditions (Article 15 Budapest Convention) than preservation, or may be visible to the suspect.

[17] The 8th Plenary adopted the report in principle subject to additional information to be provided by some Parties. It was finally adopted, following written procedure, on 25 January 2013.

5. Furthermore, greater legal certainty for preservation requests may help improve cooperation between law enforcement and service providers. Recommendation: Even if current systems allow for securing electronic evidence in an expedited manner, Parties should consider the adoption of specific provisions in their domestic legislation. Legislation should foresee that preservation requests are kept confidential by service providers or other legal or physical persons requested to preserve data.

6. The T-CY underlines in particular that preservation and data retention may be complementary tools but serve different purposes, and that data retention is therefore no substitute for data preservation.

7. The T-CY notes that in a number of Parties conditions for access to retained data are such that it is more difficult to obtain the disclosure of traffic data than more privacy-sensitive content data.

8. Some Parties are not in a position to preserve or otherwise secure electronic evidence in an expedited manner and do therefore not comply with the relevant Articles of the Budapest Convention. Recommendation: These Parties are encouraged to take urgent steps to enable their competent authorities to preserve electronic evidence in domestic and international proceedings.

9. While replies to the questionnaire confirm the importance of preservation powers, these powers are largely underused. Recommendation: Parties should therefore undertake appropriate measures to enhance their use by competent authorities. Such measures may include training and guidance notes for law enforcement on the use of preservation powers. This also applies to Articles 17 and 30 on the partial disclosure of traffic data.

10. 24/7 points of contact established under Article 35 of the Budapest Convention are a practical means to enable the sending and receiving of preservation requests (Articles 29 and 30). Replies to the questionnaire suggest that little use is made of contact points. Recommendation: Parties should take steps to inform all domestic authorities on the option of using 24/7 points of contact for urgent international cooperation in matters related to cybercrime and electronic evidence.

11. The T-CY takes note that one reason for limited use of the provisional measures of articles 29 and 30 is related to difficulties in the subsequent mutual legal assistance procedure. Recommendation: The T-CY should focus the next round of assessment in 2013 on article 31 on mutual assistance regarding accessing of stored computer data.

5.2 Summary of implementation by Parties

Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)	**Article 16 Expedited preservation**	**Article 29 Expedited preservation (international)**	**Article 17 Preservation and partial disclosure**	**Article 30 Preservation and partial disclosure (international)**
1. Albania	Y	Y	Y	Y
2. Armenia	N	N	N	N
3. Azerbaijan	P	P	Y	Y
4. Bosnia and Herzegovina	P	P	P	P
5. Bulgaria	Y	Y	Y	Y
6. Croatia	Y	Y	Y	Y
7. Cyprus	P	P	P	N
8. Denmark	No information	No information	No information	No information
9. Estonia	P	P	P	P
10. Finland	Y	Y	Y	Y
11. France	Y	Y	Y	Y
12. Georgia	P	P	P	P
13. Germany	Y	Y	P	P
14. Hungary	Y	P	P	N
15. Iceland	No information	No information	No information	No information
16. Italy	Y		Y	Y
17. Latvia	Y	Y	Y	Y
18. Lithuania	P	P	P	P
19. Republic of Moldova	P	Y	Y	Y
20. Montenegro	Y	Y	P	P
21. Netherlands	Y	Y	Y	Y
22. Norway	Y	Y	Y	Y
23. Portugal	Y	Y	Y	Y
24. Romania	Y	Y	Y	Y
25. Serbia	Y	Y	Y	Y
26. Slovakia	Y	Y	No information	No information
27. Slovenia	P	P	P	P
28. Spain	N	N	N	N
29. Switzerland	Y	Y	Y	No information
30. "The former Yugoslav Republic of Macedonia"	Y	Y	P	P
31. Ukraine	N	N	N	N
32. United Kingdom	Y	Y	Y	Y
33. United States of America	Y	Y	Y	P

5.3 Follow up

The Parties are invited to inform the Secretariat of measures taken and examples of good practices at any time.

The T-CY will review progress made within 18 months of adoption of the report (that is, by mid-2014).

6 Appendix 1: Domestic legal provisions on expedited preservation[18]

6.1 Albania

Expedited preservation:

Article 299/a Criminal Procedure Code
Expedited preservation and maintenance of the computer data
1. the prosecutor may order the expeditious preservation of certain computer data, including traffic data, when there are enough reasons to believe that the data may be lost, damaged or altered.
2. If the computer data is in the possession or control of a person, the prosecutor can order this person to preserve and maintain the integrity of the specified computer data for a period of up to 90 days, in order to search and disclose them. When there are reasonable grounds, this timeframe can be
renewed only once.
3. The person in charge of preserving and maintaining the computer data is obliged to keep confidential the procedures and actions undertaken under point 2 of this article until the end of investigations.

Law no. 9918 dated 19.05.2008 "On electronic communication"
Article 101 "Preservation and administration of data for the purpose of
criminal prosecution"
1. Regardless of other definitions in this law, the operators of networks and public electronic communications are obliged to preserve and administer the data records of their subscribers for a period of two years.
2. These records should contain data that enable:
a) The identification of subscribers ensuring the registration of their full identity
b) The identification of the end equipment used in the communication
c) the identification of the date, hour, duration of communication and the number called
3. These records should be made available, also in an electronic form, to the authorities referred to in the Criminal Procedure Code, based upon their request

Partial disclosure:

Article 299/b Criminal Procedure Code
Expedited preservation and partial disclosure of computer data
The person in charge of expeditious preservation and maintain ace of the traffic data is obliged to undertake all the necessary measures to ensure that the stored data is valid, regardless of whether one or more service providers were involved in the transmission of the communication as well as to provide the prosecutor or the authorized judicial police officer with a sufficient amount of traffic data to enable the identification of the service provider and the path through which the communication was transmitted

[18] Based on replies to questionnaire and/or Country Profiles at www.coe.int/cybercrime

6.2 Bosnia and Herzegovina

No specific legal provision. Use production order:

CPC BiH - ART. 72a
Order to the telecommunications operator
(1)If there are grounds for suspicion that a person has committed a criminal offence, on the basis of motion of the Prosecutor or officials authorized by the Prosecutor, the Court may issue an order to a telecommunications operator or another legal person performing telecommunications services to deliver information concerning the use of telecommunications services by that person, if such information could be used as evidence in the criminal proceedings or in collecting information that could be useful to the criminal proceedings.
(2)In case of emergency, the Prosecutor may order the measures under Paragraph (1) of this Article, in which case the information received shall be sealed until the issuance of the court order. The Prosecutor shall immediately inform the preliminary proceedings judge, who may issue an order within 72 hours. In case the preliminary proceedings judge does not issue the order, the Prosecutor shall return such information unsealed.
(3)Measures under Paragraph (1) of this Article may also be ordered against a person if there are grounds for suspicion that he will deliver to the perpetrator or will receive from the perpetrator information related to the offence, or grounds for suspicion that the perpetrator uses a telecommunication device belonging to this person.
(4)Telecommunications operators or other legal persons who provide telecommunications services shall enable the Prosecutor and police authorities to enforce the measures referred to in Paragraph (1) of this Article.

Similar provisions are available at entity level (CPC of RS, Art. 137 and CPC of Federation, Art. 86a).

6.3 Bulgaria

[extract from country profile 2011]

Art. 125, Art. 159, Art.162 (6), Art.163, Art. 172 (3) PPC
Chapter fourteen TECHNIQUES FOR ESTABLISHING EVIDENCE

Section III. Types of objective forms of evidence
Preparation and attachment to the case file of material evidence Article 125 (1) Where material evidence cannot be separated from the place, where it was found, and also in other cases specified by this Code, the following shall be prepared: photographs, slides, films, video tapes, sound-recordings, recordings on carriers of computerized data, layouts, schemes, casts or prints thereof.
(2) The court and the authorities entrusted with pre-trial proceedings shall also collect and inspect the objective forms of evidence prepared with the use of special intelligence means in the hypotheses herein set forth.
(3) The materials under the paragraphs 1 and 2 shall be enclosed with the case file.
Persons who shall prepare objective forms of material evidence

Section V.Searches and seizures

Obligation to hand over objects, papers, computerised data, data about subscribers to computer information service and traffic data
Article 159 Upon request of the court or the bodies of pre-trial proceedings, all institutions, legal persons, officials and citizens shall be obligated to preserve and hand over all objects, papers, computerized data, including traffic data, that may be of significance to the case.

Persons present in the course of searches and seizures
Article 162 (6) Where searches and seizures concern computerized information systems and software applications, these shall be conducted in presence of an expert- technical assistant.

Conducting searches and seizures
Article 163 (1) Searches and seizures shall be performed in daytime, except where they can suffer no delay.
(2) Before proceeding with a search and seizure, the respective body shall submit the authorisation therefore, and shall ask the objects, papers, and computerized information systems containing computerized data sought to be shown to him/her.

6.4 Croatia

Expedited preservation:

Criminal Procedure Act (Official Gazette 152/08, 76/09, 80/11)
Temporary Seizure of Objects

Article 261
(1) Objects which have to be seized pursuant to the Penal Code or which may be used to determine facts in proceedings shall be temporarily seized and deposited for safekeeping.
(2) Whoever is in possession of such objects shall be bound to surrender them upon the request of the State Attorney, the investigator or the police authorities. The State Attorney, the investigator or the police authorities shall instruct the holder of the object on consequences arising from denial to comply with the request.
(3) A person who fails to comply with the request to surrender the objects, even though there are no justified causes, may be penalized by the investigating judge upon a motion with a statement of reasons of the State Attorney pursuant to Article 259 paragraph 1 of this Act.
(4) The measures referred to in paragraph 2 of this Article shall not apply either to the defendant or persons who are exempted from the duty to testify (Article 285).

Article 263
(1) The provisions of Article 261 of this Act also apply to data saved on the computer and devices connected thereto, as well as on devices used for collecting and transferring of data, data carriers and subscription information that are in possession of the service provider, except in case when temporary seizure is prohibited pursuant to Article 262 of this Act.
(2) Data referred to in paragraph 1 of this Act must be handed over to the State Attorney upon his written request in an integral, original, legible and understandable format. The State Attorney shall stipulate a term for handing over of such data in his request. In case handing over is denied, it may be pursued in accordance with Article 259 paragraph 1 of this Act.
(3) Data referred to in paragraph 1 of this Act shall be recorded in real time by the authority carrying out the action. Attention shall be paid to regulations regarding the obligation to observe confidentiality (Articles 186 to 188) during acquiring, recording, protecting and storing of data. In accordance with the circumstances, data not related to the criminal offence for which the action is taken, and are required by the person against which the measure is applied, may be recorded to appropriate device and be returned to this person even prior to the conclusion of the proceedings.
(4) Upon a motion of the State Attorney, the investigating judge may by a ruling decide on the protection and safekeeping of all electronic data from paragraph 1 of this Article, as long as necessary and six months at longest. After this term data shall be returned, unless:

1) they are related to committing the following criminal offences referred to in the Penal Code: breach of confidentiality, integrity and availability of electronic data, programs and systems (Article 223), computer forgery (Article 223a) and computer fraud (Article 224a);

2) they are related to committing another criminal offence which is subject to public prosecution, committed by using a computer system;

3) they are not used as evidence of a criminal offence for which proceedings are instituted.

(5) The user of the computer and the service provider may file an appeal within twenty-four hours against the ruling of the investigating judge prescribing the measures referred to in paragraph 3 of this Article. The panel shall decide on the appeal within three days. The appeal shall not stay the execution of the ruling.

According to article 213. of CPA there is also possibility of evidence collecting actions before commencement of proceedings;

Article 213.

(1) The State Attorney, or the investigator upon his order, may before the commencement of the investigation, when the investigation is mandatory (Article 216 paragraph 1), conduct evidence collecting actions for which there is danger in delay, and the police may temporarily seize the items referred to in Article 261 of this Act when conducting investigation of criminal offences.

(2) If the investigation according to this Act is not mandatory, the State Attorney or the investigator upon his order, may carry out evidence collecting actions for which there is danger in delay or that are purposeful for deciding on preferring the indictment.

(3) In the case from paragraph 2 of this Article, and after receiving the instruction on the rights (Article 239), the suspect may propose evidence collecting actions to the State Attorney, and the conduct of an evidentiary hearing to the investigating judge in the cases referred to in Article 236 paragraph 2 of this Act.

(4) If a criminal charge has been filed against the defendant or he has been searched, or his home and other areas he uses and mobile objects he uses have been searched, or if an object has been temporarily confiscated from the suspect, identification conducted or fingerprints taken or prints of other body parts of the suspect, or a sample of biological material, or if an expertise of the suspect was ordered pursuant to Article 325 or 326 of this Act, the defendant may apply for the first investigation with the state attorney within 30 days from the day when criminal charge was filed or the suspect has been searched, or his home or other areas he uses or movable objects he/she uses have been searched or objects have been temporarily confiscated from the suspect, suspect identification conducted or fingerprints or prints of other body parts of the suspect taken, biological material samples taken or suspect expertise ordered pursuant to Articles 325 or 326 of this Act. If the state attorney should accept the suspect's proposal, he shall be interrogated within that term.

(5) If the state attorney has not interrogated the suspect within the term from paragraph 4 of this Article, the suspect shall have the right to review the deed upon the expiry of that term.

Special Collection of Evidence

Article 332

(1) If the investigation cannot be carried out in any other way or would be accompanied by great difficulties, the investigating judge may, upon the written request with a statement of reasons of the State attorney, order against the person against whom there are grounds for suspicion the he committed or has taken part in committing an offence referred to in Article 334 of this Act, measures which temporarily restrict certain constitutional rights of citizens as follows:

1) surveillance and interception of telephone conversations and other means of remote technical communication;

2) interception, gathering and recording of electronic data;

3) entry on the premises for the purpose of conducting surveillance and technical recording at the premises;

4) covert following and technical recording of individuals and objects;

5) use of undercover investigators and informants;

6) simulated sales and purchase of certain objects, simulated bribe-giving and simulated bribe-taking;

7) offering simulated business services or closing simulated legal business;

8) controlled transport and delivery of objects from criminal offences.

Article 333
(1) Recordings, documents and objects obtained by the application of the measures referred to in Article 332 paragraph 1 item 1 to 8 of this Act may be used as evidence in criminal proceedings.

Furthermore, Article 336 Paragraph 2. of the CPC, requires all persons who are in any way to learn about the content or actions of persons involved in implementing the actions referred to in Article 332. (Special collection of evidence), that they must keep that information secret.

Also, the CPC has a general provision on confidentiality of the investigation (Article231).

Partial disclosure:

Criminal Procedure Act (Official Gazette 152/08, 76/09, 80/11);

Article 335. par. 2.
(2) The technical operation centre for the supervision of telecommunications that carries out technical coordination with the provider of telecommunication services in the Republic of Croatia as well as providers of telecommunication services shall be bound to provide the necessary technical assistance to the police authorities. In case of proceeding contrary to this obligation, the investigating judge shall upon the motion with a statement of reasons of the State Attorney impose a fine on a provider of telecommunication services in an amount of up to HRK 1,000,000.00, and on a responsible person in the technical operative centre for the supervision of telecommunications that carries out technical coordination and on a provider of telecommunication services in the Republic of Croatia in an amount of up to HRK 50,000.00, and if thereafter the ruling is not complied with, the responsible person may be punished by imprisonment until the ruling is executed, but not longer than one month. The panel shall decide on the appeal against the ruling on the fine and imprisonment. The appeal against the ruling on the fine and imprisonment shall not stay its execution.

Decree on obligations from the area of national security of the Republic of Croatia for legal and physical persons in telecommunications (Official Gazette 64/08).

Electronic Communication Act (OG 73/08, 90/11)

6.5 Estonia

Preservation is covered by the general powers of police and prosecutor of the Criminal Procedure Code.

§ 215. Obligation to comply with orders and demands of investigative bodies and Prosecutors' Offices

(1) The orders and demands issued by investigative bodies and Prosecutors' Offices in the criminal proceedings conducted thereby are binding on everyone and shall be complied with throughout the territory of the Republic of Estonia.
(2) An investigative body conducting a criminal proceeding has the right to submit written requests to other investigative bodies for the performance of specific procedural acts and for other assistance. Such requests of investigative bodies shall be complied with immediately.
(3) A preliminary investigation judge may impose a fine of up to sixty minimum daily rates on a participant in a proceeding, other persons participating in criminal proceedings or persons not participating in the proceedings who have failed to perform an obligation provided for in subsection (1) of this section by a court ruling at the request of a Prosecutor's Office. The suspect and the accused shall not be fined.

For data retention:

Electronic Communications Act

§ 111[1]. Obligation to preserve data

(1) A communications undertaking is required to preserve the data that are necessary for the performance of the following acts:

1) tracing and identification of the source of communication;

2) identification of the destination of communication;

3) identification of the date, time and duration of communication;

4) identification of the type of communications service;

5) identification of the terminal equipment or presumable terminal equipment of a user of communications services;

6) determining of the location of the terminal equipment.

(2) The providers of telephone or mobile telephone services and telephone network and mobile telephone network services are required to preserve the following data:

1) the number of the caller and the subscriber's name and address;

2) the number of the recipient and the subscriber's name and address;

3) in the cases involving supplementary services, including call forwarding or call transfer, the number dialled and the subscriber's name and address;

4) the date and time of the beginning and end of the call;

5) the telephone or mobile telephone service used;

6) the international mobile subscriber identity (IMSI) of the caller and the recipient;

7) the international mobile equipment identity (IMEI) of the caller and the recipient;

8) the cell ID at the time of setting up the call;

9) the data identifying the geographic location of the cell by reference to its cell ID during the period for which data are preserved;

10) in the case of anonymous pre-paid mobile telephone services, the date and time of initial activation of the service and the cell ID from which the service was activated.

(3) The providers of Internet access, electronic mail and Internet telephony services are required to preserve the following data:

1) the user IDs allocated by the communications undertaking;

2) the user ID and telephone number of any incoming communication in the telephone or mobile telephone network;

3) the name and address of the subscriber to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication;

4) the user ID or telephone number of the intended recipient of an Internet telephony call;

5) the name, address and user ID of the subscriber who is the intended recipient in the case of electronic mail and Internet telephony services;

6) the date and time of beginning and end of the Internet session, based on a given time zone, together with the IP address allocated to the user by the Internet service provider and the user ID;

7) the date and time of the log-in and log-off of the electronic mail service or Internet telephony service, based on a given time zone;

8) the Internet service used in the case of electronic mail and Internet telephony services;

9) the number of the caller in the case of dial-up Internet access;

10) the digital subscriber line (DSL) or other end point of the originator of the communication.

(4) The data specified in subsections (2) and (3) of this section shall be preserved for one year from the date of the communication if such data are generated or processed in the process of provision of communications services. Requests submitted and information given pursuant to § 112 of this Act shall be preserved for two years. The obligation to preserve the information provided pursuant to § 112 rests with the person submitting the request.

(5) The data specified in subsections (2) and (3) of this section shall be preserved in the territory of a Member State of the European Union. The following shall be preserved in the territory of Estonia:
1) the requests and information provided for in § 112 of this Act;
2) the log files specified in subsection 113 (5) and the applications provided for in subsection 113 (6) of this Act;
3) the single requests provided for in § 1141 of this Act.
(6) In the interest of public order and national security the Government of the Republic may extend, for a limited period, the term specified in subsection (4) of this section.
(7) In the case specified in subsection (6) of this section the Minister of Economic Affairs and Communications shall immediately notify the European Commission and the Member States of the European Union thereof. In the absence of an opinion of the European Commission within a period of six months the term specified in subsection (4) shall be deemed to have been extended.
(8) The obligation to preserve the data provided for in subsections (2) and (3) of this section also applies to unsuccessful calls if those data are generated or processed upon providing telephone or mobile telephone services or telephone network or mobile telephone network services. The specified obligation to preserve data does not apply to call attempts.
(9) Upon preserving the data specified in subsections (2) and (3) of this section, a communications undertaking must ensure that:
1) the same quality, security and data protection requirements are met as those applicable to analogous data on the electronic communications network;
2) the data are protected against accidental or unlawful destruction, loss or alteration, unauthorised or unlawful storage, processing, access or disclosure;
3) necessary technical and organisational measures are in place to restrict access to the data;
4) no data revealing the content of the communication are preserved.
(10) The expenses related to the preserving or processing of the data specified in subsections (2) and (3) of this section shall not be compensated to communications undertakings.
(11) The data specified in subsections (2) and (3) of this section are forwarded only to a surveillance agency, a security authority, the Financial Supervision Authority or a court pursuant to the procedure provided by law.

§ 112. Obligation to provide information to surveillance agency and security authority
(1) If a surveillance agency or security authority submits a request, a communications undertaking is required to provide at the earliest opportunity, but not later than 10 hours after receiving an urgent request or within 10 working days if the request is not urgent, if adherence to the specified terms is possible based on the substance of the request, the surveillance agency or security authority with information concerning the data specified in subsections 1111 (2) and (3) of this Act.
(2) The request specified in subsection (1) of this section shall be submitted in writing or by electronic means. Requests concerning the data specified in clauses 1111(2) 1) and 2) and clause 1111 (3) 3) of the Act may also be submitted in oral form confirming the request with a password. Access to the data specified in subsection (1) of this section may be ensured, on the basis of a written contract, by way of continuous electronic connection.
(3) A communications undertaking providing mobile telephone services is required to provide a surveillance agency and security authority with real time identification of the location of the terminal equipment used in the mobile telephone network.
(4) Access to the data specified in subsection (3) of this section must be ensured on the basis of a written contract and by way of continuous electronic connection.

6.6 Finland

Budapest Convention has been implemented using similar procedure as is used with all other international conventions in Finland. This means enacting a so called "blanco" legislation (539/2007) which in a nutshell states that provisions of this convention which belong to the sphere of law in Finland are, in a manner Finland has bound itself to, in force as a law in Finland. In addition to this blanco provision also some additional provisions has been introduced into Finnish legislation. As regards article 16, the relevant national provisions which were introduced due to implementation of Budapest Convention were included in to Coercive measures Act (450/1987). Chapter 4 section 4b includes a provision on data preservation order and article 4c on duration of the data preservation order and on confidentiality. With these provisions Finnish legislation complies with articles 16 and 17 of the Convention. Unfortunately there is no English translation of these provisions (content of provisions is explained below).

The content of those provisions in essence is that (4b) If there is reason to assume that data which might have relevance in order to investigate an offence concerned will be lost or altered, an official having the competence to order an arrest may order a person holding the data to keep it unaltered. This does not apply to suspected person. A written certificate must be provided on request. These rules apply also to traffic data. Based on this preservation order, the authority does not have the right to get the information regarding the content of the data. If several service providers are involved, then the authority has the right to get the necessary traffic information in order to identify the service providers.

According to 4c, the data preservation order is ordered for fixed period of time for maximum of 3 months at a time. If the investigation requires, this period may be prolonged for maximum 3 months at a time. Person who has received the preservation order is obliged to keep it confidential. For breaching this obligation of confidentiality the penalties of chapter 38 article 1 or 2 of the criminal code applies unless a more severe punishment is provided for elsewhere in legislation.

After total reform of Coercive measures Act, these provisions on data preservation order are included in "new" Coercive measures Act (806/2011) Chapter 8, sections 24-26.

6.7 France

Pour ART. 16 (1)- ART. 56, paragraphe 7 du Code de Procédure Pénale
Avec l'accord du procureur de la République, l'officier de police judiciaire ne maintient que la saisie des objets, documents et données informatiques utiles à la manifestation de la vérité.
Le procureur de la République peut également, lorsque la saisie porte sur des espèces, lingots, effets ou valeurs dont la conservation en nature n'est pas nécessaire à la manifestation de la vérité ou à la sauvegarde des droits des personnes intéressées, autoriser leur dépôt à la Caisse des dépôts et consignations ou à la Banque de France.

ART. 60-2 du Code de Procédure Pénale, voir paragraphe 2.
L'officier de police judiciaire, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, peut requérir des opérateurs de télécommunications, et notamment de ceux mentionnés au 1 du I de l'article 6 de la loi 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant exceeder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

<u>Preservation and retention forseen in different other laws and regulations:</u>

- loi « informatique et liberté » de janvier 1978

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&fastPos=3&fastReqId=34057747&categorieLien=cid&oldAction=rechTexte

- loi sur la sécurité quotidienne du 15/11/2001, art 29
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000222052&fastPos=3&fastReqId=61552634&categorieLien=id&oldAction=rechTexte

- loi pour la confiance dans l'économie numérique de 2004, art 6
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&fastPos=5&fastReqId=347283023&categorieLien=id&oldAction=rechTexte

- décret n°2006-358 du 24 mars 2006
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000637071&fastPos=3&fastReqId=13442746&categorieLien=id&oldAction=rechTexte

- décret n°2011-219 du 25 février 2011
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023646013&fastPos=1&fastReqId=13442746&categorieLien=id&oldAction=rechTexte

6.8 Germany

German Code of Criminal Procedure (Strafprozessordnung), 2008 ("StPO"):
With respect to computer data, Article 16 is covered by Sections 94, 95 and 98 StPO.

Section 94
[Objects Which May Be Seized]
(1) Objects which may be of importance as evidence for the investigation shall be impounded or otherwise secured.
(2) Such objects shall be seized if in the custody of a person and not surrendered voluntarily.
(3) Subsections (1) and (2) shall also apply to driver's licences which are subject to confiscation.

Section 95
[Obligation to Surrender]
(1) A person who has an object of the above-mentioned kind in his custody shall be obliged to produce it and to surrender it upon request.
(2) In the case of non-compliance, the regulatory and coercive measures set out in Section 70 may be used against such person. This shall not apply to persons who are entitled to refuse to testify.

Section 98
[Order of Seizure]
(1) Seizure may be ordered only by the judge and, in exigent circumstances, by the public prosecution office and the officials assisting it (section 152 of the Courts Constitution Act). Seizure pursuant to Section 97 subsection (5), second sentence, in the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the court.
(2) An official who has seized an object without a judicial order shall apply for judicial approval within 3 days if neither the person concerned nor an adult relative was present at the time of seizure, or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may at any time apply for a judicial decision. As long as no public charges have been preferred, the decision shall be made by the court of competency pursuant to Section 162 subsection (1). Once public charges have been preferred, the decision shall be made by the court dealing with the matter. The person concerned may also submit the application to the Local Court in whose district the seizure took

place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights.

(3) Where after public charges have been preferred, the public prosecution office or one of the officials assisting has effected seizure, the court shall be notified of the seizure within 3 days; the objects seized shall be put at its disposal.
(4) If it is necessary to effect seizure in an official building or an installation of the Federal Armed Forces which is not open to the general public, the superior official agency of the Federal Armed Forces shall be requested to carry out such seizure. The necessary if the seizure is to be made in places which are inhabited exclusively by persons other than members of the Federal Armed Forces.

With respect to traffic data, Article 16 is covered by Section 100g StPO.

Section 100g

[Information on Telecommunications Connections]

(1) If certain facts give rise to the suspicion that a person, either as perpetrator, or as inciter or accessory,
1. has committed a criminal offence of substantial significance in the individual case as well, particularly one of the offences referred to in Section 100a subsection (2), or, in cases where there is criminal liability for attempt, has attempted to commit such an offence or has prepared such an offence by committing a criminal offence or
2. has committed a criminal offence by means of telecommunication;
then, to the extent that this is necessary to establish the facts or determine the accused's whereabouts, traffic data (section 96 subsection (1), section 113a of the Telecommunications Act) may be obtained also without the knowledge of the person concerned. In the case referred to in the first sentence, number 2, the measure shall be admissible only where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success and if the acquisition of the data is proportionate to the importance of the case. The acquisition of location data in real time shall be admissible only in the case of the first sentence, number 1.
(2) Section 100a subsection (3) and Section 100b subsections (1) to (4), first sentence, shall apply mutatis mutandis. Unlike Section 100b subsection (2), second sentence, number 2, in the case of a criminal offence of substantial significance, a sufficiently precise spatial and temporal description of the telecommunication shall suffice where other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or be much more difficult.
(3) If the telecommunications traffic data is not acquired by the telecommunications services provider, the general provisions shall apply after conclusion of the communication process.
(4) In accordance with Section 100b subsection (5) an annual report shall be produced in respect of measures pursuant to subsection (1), specifying:

1. the number of proceedings during which measures were implemented pursuant to subsection (1);
2. the number of measures ordered pursuant to subsection (1) distinguishing between initial orders and subsequent extension orders;
3. in each case the underlying criminal offence, distinguishing between numbers 1 and 2 of subsection (1), first sentence;
4. the number of months elapsed during which telecommunications call data was intercepted, measured from the time the order was made;
5. the number of measures which produced no results because the data intercepted was wholly or partially unavailable.

Section 100a

[Conditions regarding Interception of Telecommunications]

(1) […]

(3) Such order may be made only against the accused or against persons in respect of whom it may be assumed, on the basis of certain facts, that they are receiving or transmitting messages intended for, or transmitted by, the accused, or that the accused is using their telephone connection.

Section 100b

[Order to Intercept Telecommunications]

(1) Measures pursuant to Section 100a may be ordered by the court only upon application by the public prosecution office. In exigent circumstances, the public prosecution office may also issue an order. An order issued by the public prosecution office shall become ineffective if it is not confirmed by the court within 3 working days. The order shall be limited to a maximum duration of 3 months. An extension by not more than 3 months each time shall be admissible if the conditions for the order continue to apply taking into account the existing findings of the enquiry.

(2) The order shall be given in writing. The operative part of the order shall indicate:

1. where known, the name and address of the person against whom the measure is directed,
2. the telephone number or other code of the telephone connection or terminal equipment to be intercepted, insofar as there are no particular facts indicating that they are not at the same time assigned to another piece of terminal equipment.
3. the type, extent and duration of the measure specifying the time at which it will be concluded.

(3) On the basis of this order all persons providing, or contributing to the provision
of, telecommunications services on a commercial basis shall enable the court, the public prosecution office and officials working in the police force to assist it (section 152 of the Courts Constitution Act), to implement measures pursuant to Section 100a and shall provide the required information without delay. Whether and to what extent measures are to be taken in this respect shall follow from the Telecommunications Act and from the Telecommunications Interception Ordinance issued thereunder. Section 95 subsection (2) shall apply mutatis mutandis.

(4) If the conditions for making the order no longer prevail, the measures implemented on the basis of the order shall be terminated without delay. Upon termination of the measure, the court which issued the order shall be notified of the results thereof.

(5) […]

6.9 Georgia

Article 111. General Rule for Conducting Investigative Actions

1. The parties have equal rights and obligations during the conduct of investigative actions according to the rule established by this Code except the cases determined under paragraph 2 of this article. The parties conduct investigative actions according to the rule established by this Code and within its frames. A prosecutor is authorized to attend the investigative action conducted by the law enforcement institutions. The law enforcement institutions shall not conduct investigative actions without the participation of a prosecutor if he/she demands so. A prosecutor shall be entitled to be present at the investigative action carried out by the defense, with the consent of the defense.

2. A defense is not authorized to submit a motion to a court for conduct of search and seizure.

3. Prior to launching an investigative action, a person carrying out an investigative action shall explain to the participants their rights and duties, and the rules for conducting an investigative action. The person conducting an investigative action is required to ensure that the involved parties have opportunity to exercise their rights.

4. If an investigator's ruling or a court order authorizes an investigative action, the investigator shall under signature present the ruling (court order) to the person required to fulfill it.

5. It shall be impermissible to carry out the investigative action at night, except in cases of urgency. An investigative action shall be conducted within a reasonable time.

6. Scientific-technical means and methods for discovering, securing, and extracting trace evidence and physical evidence may be used during investigative action.

7. In case of resistance toward an investigative action, a proportionate compulsory measure may be applied.

8. During an investigative action, it shall only be permissible to apply surgical, or other methods and means of medical examination, that cause considerable pain, in exceptional cases , with the consent of a person to be examined; if a person to be examined is under 16 years of age or he/she is mentally ill, with the consent of a parent, guardian or custodian, or by a court order.

9. If a conduct of an investigative activity requires special professional skills, a party shall conduct it with participation of an expert. If an investigative activity requires that an individual to be undressed, upon to the his/her request, an expert and a party shall be of the same sex as the person under examination.

Article 112. Investigative Action Conducted on the Basis of a Court Order

1. An investigative action related to the restriction of one's private property, ownership or right to privacy of a dwelling, shall be carried out on the basis of a court order issued on the motion of the parties. A judge shall without the oral hearing decide on the motion within 24 hours from the moment of receiving a motion and other necessary information for reviewing the motion. A judge shall be authorized to consider the motion with participation of the party filing the motion. In this case rules for considering motions set forth in Article 206 of this Code shall apply. Consent of co-owner or one party to communication is sufficient to conduct investigative actions without the court order determined under this paragraph.

2. The court order shall contain the date and the place of its drafting, the last name of the judge, the person filing a motion, the order to carry out an investigative action, indicating its purpose and addressee, the term of the order's validity, a person or a body required to fulfill the order, and the judge's signature (including electronic signature). (2011.05.05)

3. The court order concerning search or seizure shall also indicate: the movable and immovable property, where the investigative action shall be permitted and person who owns it (if such person is identified), a natural person to be searched; an item, thing, substance, or any other object likely to be uncovered and seized during the search and seizure and its general characteristics; the right to apply an appropriate compulsory measure in case of resistance. A court order on search or seizure shall be invalid if such investigative action has not commenced within 30 days.

4. The order concerning arrest and seizure of a postal-telegraphic message made through the technical means of communication shall also include: the name and surname of the recipient of a message; the name, surname, and address of a person sending a message (if such information is available); a type of postal-telegraphic message to be arrested; the term of arrest; a title of a postal-telegraphic institution required to arrest a postal-telegraphic message; and the right of an investigator to examine and seize the postal-telegraphic message.

5. The investigative action referred to in Paragraph 1 of this article may be conducted without a court order, upon an investigator's ruling, in case of urgency, where delay may cause the destruction of factual data essential for the case or will make it impossible to obtain such data, or when an object, document, substance or any other object containing information is discovered during another investigative action (plain view concept), or when a real threat to a person's health or life exists. In this case a prosecutor shall notify a judge, having jurisdiction over the territory where the investigative action has been carried out, or a judge having jurisdiction over the place of investigation, within 24 hours from the moment of starting an investigative activity and shall transfer a file or a criminal case (or copies thereof) that justify the necessity of taking urgent investigative actions. A judge shall make a decision on a motion without an oral hearing within 24 hours from receiving the materials. The judge shall be authorized to consider a motion with participation of the parties (if the criminal prosecution has begun), as well as with participation of the person, against whom the investigative action has been conducted. While considering a motion a judge shall probe the legitimacy of the investigative action carried out without a court decision. A judge shall be authorized to summon a person who conducted the investigative action without a court order for obtaining explanations from the person. In this case rules for considering motions set forth in Article 206 of this Code shall apply.

6. After examining the case materials a court shall render an order on:

a) finding the investigative action legitimate;

b) finding the investigative action illegitimate and the collected information to be inadmissible evidence.

7. The judge has the right to consider the matters under this Article without an oral hearing.

8. The order issued pursuant to this article may be appealed in accordance with the rules set forth in the article 207 of this Code. The term for appeal shall be calculated from the enforcement of an order.

Article 119. The Purpose and Grounds for Search and Seizure

1. If there is a probable cause, a search and seizure shall aim at uncovering and seizure of any object, document, substance, or other item that contains information related to the case.

2. It is also permissible to conduct a search for a fugitive and/or for recovery of a corpse.

3. An object, document, or other item including information relevant to the case may be seized if a there is a probable cause that the object, document, or other item is kept in a certain place, with a certain person, and if it is not necessary to search for them.

4. It shall be possible to conduct a search for a seizure of an object, document, or other item including information relevant to a certain case, if there is a probable cause, that it is kept in a certain place, with a certain person, and if search is necessary for discovering it.

Article 120. The Rule for Search and Seizure

1. On the basis of a court order or in case of urgency – on the basis of ruling – authorizing search or seizure, an investigator shall have the right to enter storage, dwelling, or other ownership for the discovery and seizure of an object, document, or other item containing relevant information for the case.

2. Prior to a search or a seizure the investigator shall be obliged to present a court order or in case of urgency – a ruling, to a person subject to search and seizure. The presentation of the order (ruling) shall be confirmed by the signature of the person.

3. While the search/seizure is being conducted, an investigator shall have the right to restrict the person(s) at the place of search/seizure from leaving and from communicating with one another or with other persons. This shall be reflected in the relevant record.

4. Upon presenting a court order, in case of urgency – ruling, the investigator shall offer the person subject to search or seizure to voluntarily turn over the object, document, or other item containing relevant information. If the item to be seized is voluntarily turned over, it shall be noted in the record; in case of refusal to turn over the requested items voluntarily or in case of partial disclosure the seizure by coercion shall take place.

5. During the search the object, document, substance, or other item containing information, which is indicated in the court order or ruling shall be searched for and seized. Any other object containing information that might have an evidentiary value on the concerned case or that might clearly indicate on other crime, as well as the objects, substances and/or other items removed from the circulation may also be seized.

6. All items containing information, all objects, documents, substances, or other relevant items discovered during the search or seizure shall be presented to the persons participating in the investigative action if possible prior to the seizure. Upon the presentation, they shall be seized, described in detail, sealed, and packaged, if possible. Apart from the seal, the packaged items shall reflect the date and signatures of the persons participating in the investigative action.

7. During the search and seizure the investigator shall have the right to open a closed storage or premise if the person to be searched refuses to do so voluntarily.

8. If there is a probable cause that the persons present at the place of search or seizure have hidden the object, document, substance, or other item to be seized, personal search of such person shall be allowed. Such case shall be regarded as urgent necessity and, shall be conducted without a court order or a investigator's ruling. The legitimacy of search and/or seizure shall be reviewed by the court in accordance with the rules established by this Code.

9. Search or seizure in the building of a legal entity or an administrative body shall take place in the presence of the head or a representative of that entity or the body.

Article 136. Request for document or information

1. If there is a probable cause that the information or document important for the criminal case is kept in a computer system or data storage, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting relevant information or document.

2. If there is a probable cause that a person commits a crime though a computer system, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting a service provider to submit existed subscriber information.

3. For the purpose of this Article, subscriber information means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be determined:

a) the type of communication service used, the technical provisions taken thereto and the period of service;

b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, which is available on the basis of the service agreement or arrangement;

c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

4. Motions provided by paragraph 1 and 2 of this Article, shall be considered by the court in accordance with the procedure established by Article 112 of the present Code.

Law of Georgia on Operative-Investigative Activity

Article 7. Definition of Operative-Investigative Activity

1. Operative-Investigative Activity is an activity of the authorized public agency or an official determined by the Law, who ensures performance of the goals provided by Article 2 of the present Law within its competence.

2. For the performance of these goals an authorized public agencies openly or through preserving conspiracy rules use:

[…]

h) Hidden recording of or eavesdropping on telephone conversation, receiving information and fixing from transmission lines (though connection to transmission means, computer networks, streamline communication), from computer system (directly or remotely) and for this purpose installation of relevant software devices; control of postal and telegraphic parcels (except diplomatic post) based on the order of the court.

[…]

6.10 Hungary

Criminal Procedure Act

ORDER TO RESERVE COMPUTER DATA

Section 158/A (1) Compulsion to reserve data means the temporary restriction of the right of disposal of a person possessing, processing or managing data recorded by a computer system (hereinafter: computer data) over specific computer data, in order to investigate and prove a criminal offence.
(2) The court, the prosecutor or the investigating authority shall order the reservation of computer data constituting a means of evidence or required to trace any means of evidence or the establishment of the identity or location of a suspect.
(3) From the time of being notified of the order, the obliged party shall reserve the data recorded by the computer system designated in the order, and ensure its safe storage, if necessary, separately from other data files. The obliged party shall prevent the modification, deletion, destruction of the computer data, as well as the transmission and unauthorised copying thereof and unauthorised access thereto.
(4) The party ordering the reservation of data may affix its advanced electronic signature on the data to be reserved. If the reservation of the data at its original location considerably hindered the activity of the obliged party to process, manage, store or transmit data, the obliged party may, with the permission of the issuer of the order, ensure reservation by copying the data into another data medium or computer system. After the copy has been made, the issuer of the order may wholly or partially relieve the restrictions concerning the data medium and computer system holding the original data.
(5) While the measure is in effect, the data to be reserved may solely be accessed by the court, prosecutor or investigating authority having issued the order, and – with their respective permission – the person possessing or managing the data. The person possessing or managing the data to be reserved may only provide information of such data with the express permission of the issuer of the order during the effect of the measure.
(6) The obliged party shall forthwith notify the issuer of the order if the data to be reserved has been modified, deleted, copied, transmitted or viewed without authorisation, or an indication of an attempt of the above has been observed.
(7) After issuing the order for reservation, the issuer shall start to review the affected data without delay, and depending on its findings, and either order the seizure of the data by copying them to the computer system or other data medium, or terminate the order for their reservation.
(8) The obligation to reserve data shall be in effect until the seizure of the data, but no longer than for three months. The obligation to reserve the data shall terminate if the criminal proceeding has been concluded. The obliged party shall be advised of the conclusion of the criminal proceeding.

6.11 Italy

Art. 132, paragraph 4ter and 4quater D. Lgs. 196/2003 (Data Protection Act)

Art. 132. Conservazione di dati di traffico per altre finalità 4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonchè gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.

[Internet translation only: Art. 132. Preservation of traffic data for other purposes 4-ter. The Minister of the Interior or his delegate, on the central offices responsible for specialized computer or telematics matters of State police, the carabinieri and the guardia di finanza and the other persons referred to in paragraph 1 of article 226 of the implementing rules, coordination and transitional provisions of the code of criminal procedure, referred to in Legislative Decree July 28, 1989No. 271, they can order, including in relation to any requests made by foreign investigative authorities, operators and suppliers of services or telecommunication to preserve and protect, in accordance with the procedures laid down and for a period not exceeding ninety days, traffic data, excluding however the contents of communications, for the purpose of carrying out pre-emptive investigations provided for in article 226 of the mentioned rules laid down in Legislative Decree No. 271 of 1989— for purposes of detection and suppression of specific crimes. The measure, which may be extended, for motivated needs a total duration not exceeding six months may provide particular data storage mode and the possible unavailability of data from suppliers and operators of computer or telematic services or third parties.]

Law 28 of 18 March 2008[19] modified or introduced a range of provisional measures in the Code of Criminal Procedure, including:

Art. 244. Casi e forme delle ispezioni.
1. L'ispezione delle persone, dei luoghi e delle cose è disposta con decreto motivato quando occorre accertare le tracce e gli altri effetti materiali del reato.
2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. ([1])
(1) Parole aggiunte dall'art. 8, comma 1, della L. 18 marzo 2008, n. 48.

Art. 247. Casi e forme delle perquisizioni.
1. Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in

[19] This law was enacted in view of ratification of the Budapest Convention on Cybercrime by Italy.

un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.
1-bis. Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorchè protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione. ([1])
2. La perquisizione è disposta con decreto motivato.
3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.
(1) Comma inserito dall'art 8, comma 2, della L 18 marzo 2008, n. 48

Art. 248. Richiesta di consegna.
1. Se attraverso la perquisizione si ricerca una cosa determinata, l'autorità giudiziaria può invitare a consegnarla. Se la cosa è presentata, non si procede alla perquisizione, salvo che si ritenga utile procedervi per la completezza delle indagini.
2. Per rintracciare le cose da sottoporre a sequestro o per accertare altre circostanze utili ai fini delle indagini, l'autorità giudiziaria o gli ufficiali di polizia giudiziaria da questa delegati possono esaminare presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici. ([1]) In caso di rifiuto, l'autorità giudiziaria procede a perquisizione.
(1) Parole così modificate dall'art. 8, comma 3, della L. 18 marzo 2008, n. 48.

Art. 254. Sequestro di corrispondenza.
1. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato. ([1])
2. Quando al sequestro procede un ufficiale di polizia giudiziaria, questi deve consegnare all'autorità giudiziaria gli oggetti di corrispondenza sequestrati, senza aprirli o alterarli e senza prendere altrimenti conoscenza del loro contenuto.
3. Le carte e gli altri documenti sequestrati che non rientrano fra la corrispondenza sequestrabile sono immediatamente restituiti all'avente diritto e non possono comunque essere utilizzati.
(1) Articolo così modificato dall'art. 8, comma 3, della L 18 marzo 2008, n. 48.

Art. 254-bis. Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni. ([1])
1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.
(1) Articolo inserito dall'art. 8, comma 5, della L 18 marzo 2008, n. 48

Art. 256. Dovere di esibizione e segreti.
1. Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, ([1]) e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di segreto di Stato ovvero di segreto inerente al loro ufficio o professione.
2. Quando la dichiarazione concerne un segreto di ufficio o professionale, l'autorità giudiziaria, se ha motivo di dubitare della fondatezza di essa e ritiene di non potere procedere senza acquisire gli atti, i documenti o le

cose indicati nel comma 1, provvede agli accertamenti necessari. Se la dichiarazione risulta infondata, l'autorità giudiziaria dispone il sequestro.
3. Quando la dichiarazione concerne un segreto di Stato, l'autorità giudiziaria ne informa il Presidente del Consiglio dei Ministri, chiedendo che ne sia data conferma. Qualora il segreto sia confermato e la prova sia essenziale per la definizione del processo, il giudice dichiara non doversi procedere per l'esistenza di un segreto di Stato.
4. Qualora, entro sessanta giorni dalla notificazione della richiesta, il Presidente del Consiglio dei Ministri non dia conferma del segreto, l'autorità giudiziaria dispone il sequestro.
5. Si applica la disposizione dell'articolo 204.
(1) Le parole: "*nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto*" sono state inserite dall'art. 8, comma 6, della L. 18 marzo 2008, n. 48.

Art. 259. Custodia delle cose sequestrate.
1. Le cose sequestrate sono affidate in custodia alla cancelleria o alla segreteria. Quando ciò non è possibile o non è opportuno, l'autorità giudiziaria dispone che la custodia avvenga in luogo diverso, determinandone il modo e nominando un altro custode, idoneo a norma dell'articolo 120.
2. All'atto della consegna, il custode è avvertito dell'obbligo di conservare e di presentare le cose a ogni richiesta dell'autorità giudiziaria nonché delle pene previste dalla legge penale per chi trasgredisce ai doveri della custodia. Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria. ([1]) Al custode può essere imposta una cauzione. Dell'avvenuta consegna, dell'avvertimento dato e della cauzione imposta è fatta menzione nel verbale. La cauzione è ricevuta, con separato verbale, nella cancelleria o nella segreteria.
(1) Periodo inserito dall'art. 8, comma 7, della L. 18 marzo 2008, n. 48.

Art. 260. Apposizione dei sigilli alle cose sequestrate. Cose deperibili.
1. Le cose sequestrate si assicurano con il sigillo dell'ufficio giudiziario e con le sottoscrizioni dell'autorità giudiziaria e dell'ausiliario che la assiste ovvero, in relazione alla natura delle cose, con altro mezzo, anche di carattere elettronico o informatico ([1]), idoneo a indicare il vincolo imposto a fini di giustizia.
2. L'autorità giudiziaria fa estrarre copia dei documenti e fa eseguire fotografie o altre riproduzioni delle cose sequestrate che possono alterarsi o che sono di difficile custodia, le unisce agli atti e fa custodire in cancelleria o segreteria gli originali dei documenti, disponendo, quanto alle cose, in conformità dell'articolo 259. Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria. ([2])
3. Se si tratta di cose che possono alterarsi, l'autorità giudiziaria ne ordina, secondo i casi, l'alienazione o la distruzione.
3-bis. L'autorità giudiziaria procede, altresì, anche su richiesta dell'organo accertatore alla distruzione delle merci di cui sono comunque vietati la fabbricazione, il possesso, la detenzione o la commercializzazione quando le stesse sono di difficile custodia, ovvero quando la custodia risulta particolarmente onerosa o pericolosa per la sicurezza, la salute o l'igiene pubblica ovvero quando, anche all'esito di accertamenti compiuti ai sensi dell'articolo 360, risulti evidente la violazione dei predetti divieti. L'autorità giudiziaria dispone il prelievo di uno o più campioni con l'osservanza delle formalità di cui all'articolo 364 e ordina la distruzione della merce residua. ([3])
3-ter. Nei casi di sequestro nei procedimenti a carico di ignoti, la polizia giudiziaria, decorso il termine di tre mesi dalla data di effettuazione del sequestro, può procedere alla distruzione delle merci contraffatte sequestrate, previa comunicazione all'autorità giudiziaria. La distruzione può avvenire dopo 15 giorni dalla comunicazione salva diversa decisione dell'autorità giudiziaria. E' fatta salva la facoltà di conservazione di campioni da utilizzare a fini giudiziari. ([3])

(1) Parole inserite dall'art. 8, comma 8, lett. a) della L. 18 marzo 2008, n. 48
(2) Periodo inserito dall'art. 8, comma 8, lett. b) della L. 18 marzo 2008, n. 48.
(3) Comma inserito dall'art. 2, comma 1, lett. a) del D.L. 23 maggio 2008, n. 92

Art. 352. Perquisizioni.

1. Nella flagranza del reato o nel caso di evasione, gli ufficiali di polizia giudiziaria procedono a perquisizione personale o locale quando hanno fondato motivo di ritenere che sulla persona si trovino occultate cose o tracce pertinenti al reato che possono essere cancellate o disperse ovvero che tali cose o tracce si trovino in un determinato luogo o che ivi si trovi la persona sottoposta alle indagini o l'evaso.
1-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorche protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi. ([1])
2. Quando si deve procedere alla esecuzione di un'ordinanza che dispone la custodia cautelare o di un ordine che dispone la carcerazione nei confronti di persona imputata o condannata per uno dei delitti previsti dall'articolo 380 ovvero al fermo di una persona indiziata di delitto, gli ufficiali di polizia giudiziaria possono altresì procedere a perquisizione personale o locale se ricorrono i presupposti indicati nel comma 1 e sussistono particolari motivi di urgenza che non consentono la emissione di un tempestivo decreto di perquisizione.
3. La perquisizione domiciliare può essere eseguita anche fuori dei limiti temporali dell'articolo 251 quando il ritardo potrebbe pregiudicarne l'esito.
4. La polizia giudiziaria trasmette senza ritardo, e comunque non oltre le quarantotto ore, al pubblico ministero del luogo dove la perquisizione è stata eseguita il verbale delle operazioni compiute. Il pubblico ministero, se ne ricorrono i presupposti, nelle quarantotto ore successive, convalida la perquisizione.
(1) Comma inserito dall'art. 9, comma 1, della L. 18 marzo 2008, n. 48.

Art. 353. Acquisizione di plichi o di corrispondenza.

1. Quando vi è necessità di acquisire plichi sigillati o altrimenti chiusi, l'ufficiale di polizia giudiziaria li trasmette intatti al pubblico ministero per l'eventuale sequestro.
2. Se ha fondato motivo di ritenere che i plichi contengano notizie utili alla ricerca e all'assicurazione di fonti di prova che potrebbero andare disperse a causa del ritardo, l'ufficiale di polizia giudiziaria informa col mezzo più rapido il pubblico ministero il quale può autorizzarne l'apertura immediata e l'accertamento del contenuto. ([1])
3. Se si tratta di lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica, ([2]) per i quali è consentito il sequestro a norma dell'articolo 254, gli ufficiali di polizia giudiziaria, in caso di urgenza, ordinano a chi è preposto al servizio postale, telegrafico, telematico o di telecomunicazione ([3]) di sospendere l'inoltro. Se entro quarantotto ore dall'ordine della polizia giudiziaria il pubblico ministero non dispone il sequestro, gli oggetti di corrispondenza sono inoltrati.
(1) Le parole: "*e l'accertamento del contenuto*" sono state aggiunte dall'art. 9, comma 2, lett. a), della L. 18 marzo 2008, n. 48
(2) Le parole: "*lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica*" sono state aggiunte dall'art. 9, comma 2, lett. b) della L. 18 marzo 2008, n. 48
(3) Le parole: "*telegrafico, telematico o di telecomunicazione*" sono state aggiunte dall'art. 9, comma 2, lett. b) della L. 18 marzo 2008, n. 48

Art. 354. Accertamenti urgenti sui luoghi, sulle cose e sulle persone. Sequestro.

1. Gli ufficiali e gli agenti di polizia giudiziaria curano che le tracce e le cose pertinenti al reato siano conservate e che lo stato dei luoghi e delle cose non venga mutato prima dell'intervento del pubblico ministero.
2. Se vi è pericolo che le cose, le tracce e i luoghi indicati nel comma 1 si alterino o si disperdano o comunque si modifichino e il pubblico ministero non può intervenire tempestivamente, ovvero non ha ancora assunto la direzione delle indagini, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sullo stato dei luoghi e delle cose. In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità. ([1]) Se del caso, sequestrano il corpo del reato e le cose a questo pertinenti.
3. Se ricorrono i presupposti previsti dal comma 2, gli ufficiali di polizia giudiziaria compiono i necessari accertamenti e rilievi sulle persone diversi dalla ispezione personale. ([2])
(1) Il periodo che recita: "*In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità*" è stato inserito dall'art. 9, comma 3, della L. 18 marzo 2008, n. 48
(2) Il periodo che recita: "*Se gli accertamenti comportano il prelievo di materiale biologico, si osservano le disposizioni del comma 2-bis dell'articolo 349.*" è stato soppresso dall'art. 27 della L. 30 giugno 2009, n. 85

6.12 Latvia

Expedited preservation

Latvian Criminal procedure law, Section 191. "Storage of Data located in an Electronic Information System":

- a person directing the proceedings may assign, with a decision thereof, the owner, possessor or keeper of an electronic information system (that is, a natural or legal person who processes, stores or transmits data via electronic information systems, including a merchant of electronic communications) to immediately ensure the storage, in an unchanged state, of the totality of the specific data (the retention of which is not specified by law) necessary for the needs of criminal proceedings that is located in the possession thereof, and the inaccessibility of such data to other users of the system.
- the duty to store data may be specified for a term of up to thirty days, but such term may be extended, if necessary, by an investigating judge by a term of up to thirty days.

Partial disclosure

Criminal procedure law, Section 192 "Disclosure and Issue of Data Stored in an Electronic Information System":
(2) During the pre-trial criminal proceedings the person directing the proceedings may request in writing, based on a decision of an investigating judge or with the consent of a data subject, that the owner, possessor or keeper of an electronic information system disclose and issue the data stored in accordance with the procedures provided for in Section 191 of this Law.

6.13 Lithuania

National laws and other legal acts of the Republic of Lithuania allowing for the Lithuanian police to apply expedited preservation of stored computer data in the Lithuania are as follows:

1. The **Law on the Electronic Communications** of the Republic of Lithuania, No. IX-2135, 15 April 2004 (Official Gazette, No. 69-2382, 2004) (hereinafter referred to as "the **LEC**").

   The **LEC** regulates social relations pertaining to electronic communications services and networks, associated facilities and services, use of electronic communications resources as well as social relations pertaining to radio equipment, terminal equipment and electromagnetic compatibility.

   Article 65 Paragraph 2 of the **LEC** provides that in order to ensure accessibility of data for the purposes of investigation, disclosure and persecution of serious and grave crimes specified in the Criminal Code of the Republic of Lithuania, providers of a public communications network and/or public electronic communications services must preserve and submit free of charge to the competent institutions, in accordance with the procedure established by the law, generated or processed data indicated in the Annex 1 "Categories of Data to be Stored" of the LEC (see below):

   „Categories Of Data To Be Stored

   1. Data necessary to trace and identify the source of a communication:
   1.1. Data concerning fixed network telephony and mobile telephony:
   1.1.1. the calling telephone number;
   1.1.2. name, surname and address of the subscriber or registered user of electronic communications services;
   1.2. Data concerning Internet access, Internet e-mail and Internet telephony:
   1.2.1. the user ID(s) allocated;
   1.2.2. the user ID and telephone number allocated to any communication entering the public telephone network;
   1.2.3. the name and address of the subscriber or registered user to whom an Internet Protocol (IP) address, user ID or telephone number was allocated at the time of the communication.

   2. Data necessary to identify the destination of a communication:
   2.1. Data concerning fixed network telephony and mobile telephony:
   2.1.1. the number(s) dialled (the telephone number(s) called), and, in cases involving supplementary services such as call forwarding or call transfer, the number or numbers to which the call is routed;
   2.1.2. the name(s) and address(es) of the subscriber(s) or registered user(s);
   2.2. Data concerning Internet e-mail and Internet telephony:
   2.2.1. the user ID or telephone number of the intended recipient(s) of an Internet telephony call;
   2.2.2. the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication.

   3. Data necessary to identify the date, time and duration of communication:
   3.1. Data concerning fixed network telephony and mobile telephony, the date and time of the start and end of the communication;
   3.2. Data concerning Internet access, Internet e-mail and Internet telephony:
   3.2.1. the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with the IP address, whether dynamic or static, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

3.2.2. the date and time of the log-in and log-off of the Internet e-mail service or Internet telephony service, based on a certain time zone.

4. Data necessary to identify the type of communication:
4.1. Data concerning fixed network telephony and mobile telephony: the telephone service used;
4.2. Data concerning Internet e-mail and Internet telephony: the Internet service used.

5. Data necessary to identify users' communication equipment or what purports to be their equipment:
5.1. Data concerning fixed network telephony, the calling and called telephone numbers;
5.2. Data concerning mobile telephony:
5.2.1. the calling and called telephone numbers;
5.2.2. the International Mobile Subscriber Identity (IMSI) of the calling party;
5.2.3. the International Mobile Equipment Identity (IMEI) of the calling party;
5.2.4. the IMSI of the called party;
5.2.5. the IMEI of the called party;
5.2.6. in the case of pre-paid anonymous services, the date and time of the initial activation of the service and the location label (Cell ID) from which the service was activated;
5.3. concerning Internet access, Internet e-mail and Internet telephony:
5.3.1. the calling telephone number for dial-up access;
5.3.2. the digital subscriber line (DSL) or other end point of the originator of the communication.
6. data necessary to identify the location of mobile communication equipment:
6.1. the location label (Cell ID) at the start of the communication;
6.2. data identifying the geographic location of cells by reference to their location labels (Cell ID) during the period for which communications data are retained."

The data listed in the 1 Annex above, according to Article 66 Paragraph 6 of the **LEC** shall be stored by the providers for 6 months from the date of the communication.

According to Article 66 Paragraph 8 of the **LEC**, providers of a public communications network and/or public electronic communications services must store data in accordance with the following principles:

"1) the data must be of the same quality and subject to the same security and protection as the network data;
2) the data shall be subject to appropriate technical and organizational measures to protect data against accidental or unlawful destruction or accidental loss or alteration, unauthorized or unlawful storage, processing, use or disclosure;
3) the data shall be subject to appropriate technical and organizational measures to ensure that access to them could get only by authorized personnel."

2. The **Law on Operational Activities** of the Republic of Lithuania, No IX-965, 20 June 2002 (Official Gazette No. 65-2633, 2002) (as last amended on 27 March 2012, No. XI-1941, Official Gazette No. 42-2043, entered into force since 7 April, 2012) (hereinafter referred to as "the **LOA**").

The LOA regulates the legal basis for operational activities, principles and tasks of operational activities, the rights and duties of entities of operational activities, the carrying out of operational actions and operational investigation, participation of persons in operational activities, the use and disclosure of operational intelligence as well as the financing, control, and scrutiny of these activities.

/.../
8. **Use of technical means in operational activities** shall mean the installation, operation or dismantling of technical means and other lawful actions related thereto. Technical means may be used in operational activities in accordance with the general and special procedure.
9. **Use of technical means in accordance with the special procedure** shall mean the use of technical means in operational activities authorised by a reasoned court ruling when monitoring or recording personal conversations, other communications or actions, where none of the participants in the conversation, other communications or actions is aware of such monitoring and it is implemented by restricting the individual's right to inviolability of private life in accordance with the procedure laid down by law. The monitoring of the content and recording of the personal information transmitted by electronic communications networks, even if one of the persons is aware of such control, shall be subject to a reasoned court ruling, with the exception of the cases when a person requests or consents to such monitoring or recording without making use of the services and equipment of the economic entities providing the electronic communications networks and/or services.
/.../
24. **Operational investigation** shall mean an organisational tactical form of operational activities covering operational actions, including the actions requiring a reasoned court ruling or a prosecutor's authorisation. In carrying out an operational investigation, entities of operational activities may process operational investigation files."

Article 7 Paragraph 4 of the **LOA** provides rights of entities of operational activities:

"4. Entities of operational activities shall, on the grounds for an operational investigation provided for in Article 9 of this Law and upon obtaining the authorisation specified in Articles 10, 11, 12 or 13 of this Law, have the right:
1) to covertly monitor postal items, document items, money orders and documents thereof, obtain information on the economic, financial operations of a natural or legal person and on the use of financial instruments and/or means of payment;
2) to use technical means and obtain information from the economic entities providing electronic communications networks and/or services in accordance with the special procedure;
3) in accordance with the procedure laid down by the Government upon co-ordination with the Bank of Lithuania, to obtain information from the Bank of Lithuania; to obtain information from commercial banks, other credit and financial institutions, also from other legal persons – in accordance with the procedure laid down by the Government;
4) to covertly enter residential and non-residential premises and vehicles and to inspect them, to temporarily seize and inspect documents, seize samples of substances, raw materials and production as well as other objects for investigation without disclosing the fact of seizure thereof;
5) to use the mode of conduct imitating a criminal act;
6) to carry out controlled delivery."

Article 9. Grounds for an Operational Investigation
An operational investigation shall be conducted, when:
1) characteristics of a criminal act have not been established, but information is available about a **grave** or **serious crime** being planned, being committed or having been committed or **less serious** crimes provided for in Article 131, paragraph 2 of Article 145, paragraphs 2 and 3 of Article 146, paragraph 2 of Article 151, Article 162, paragraph 2 of Article 178, paragraph 1 of Article 180, paragraph 1 of Article 181, paragraph 2 of Article 187, paragraph 2 of Article 189, paragraph 1 of Article 189[1], paragraph 2 of Article 198, paragraph 1 of Article 213, Articles 214 and 215, paragraph 1 of Article 225, paragraphs 1 and 2 of Article 226, paragraphs 1 and 2 of Article 227, paragraph 1 of Article 228, Article 228[1], Article 240, paragraph 1 of Article 253, paragraph 1 of Article 256, paragraphs 2 and 3 of Article 300, paragraph 2 of Article 301, paragraph 2 of Article 302 and paragraphs 1 and 2 of Article 307 of the

Criminal Code of the Republic of Lithuania or about a person planning, committing or having committed a crime;
2) information is available about the activities of the special services of other states;
3) the suspect, the accused or the convicted person goes into hiding;
4) a person is reported missing;
5) protection of persons against criminal influence is being implemented;
6) protection of state secrets is being implemented;
7) information is available about the acts positing a threat to the constitutional system of the State, independence and economic security thereof, ensuring of the defence power of the State or other interests of importance to national security."

Article 10. Covert Monitoring of Postal Items, Document Items, Money Orders and Documents Thereof, Use of Economic, Financial Operations of a Natural or Legal Person, Financial Instruments and/or Means of Payment, Use of Technical Means in Accordance with the Special Procedure and Obtaining of Information from the Economic Entities Providing Electronic Communications Networks and/or Services, from the Bank of Lithuania, Commercial Banks, Other Credit and Financial Institutions, Also from Other Legal Persons
.....

3. The **Criminal Code** of the Republic of Lithuania, approved by the Law of the Republic of Lithuania No. VIII-1968, 26 September, 2000 (Official Gazette, No. 89-2741, No. 46, 2000) (as last amended by the Law No. XI-1861, 22 December, 2011, Official Gazette, No. 5-138, 2012, entered into force since 7 January, 2012) (hereinafter referred to as "the **CC**").

4. The **Code of the Criminal Procedure** of the Republic of Lithuania, approved by the Law of the Republic of Lithuania No. IX-785, 14 March, 2002 (Official Gazette, No. 37-1341, No. 46, 2002) (as last amended by the Law No. XI-1478, 21 June, 2011, Official Gazette, No. 81-3965, 2011, entered into force since 5 July, 2011) (hereinafter referred to as "the **CCP**").

The **CCP** regulates social relations pertaining to pre-trial investigations of criminal acts as well as proceedings in the criminal courts.

Article 154 of the **CCP** provides coercive investigative measure – the seizure of items, which are presumed to be evidences in the court:

"Article 147. Seizure
1. When it is necessary to obtain items or documents important for investigation of a criminal act and location or possessor thereof is known a pre-trial investigation officer or prosecutor may implement seizure. Seizure is imposed by a grounded ruling of a pre-trial investigation judge. In cases of emergency seizure can be implemented by a decision of a pre-trial investigation officer or prosecutor however, in such a case approval of a pre-trial investigation judge in respect of the implemented seizure shall be acquired within three days from the day of actual seizure. Upon failure to acquire approval of a pre-trial investigation judge within said term all the seized items and documents shall be returned to the persons from whom they were seized and the results of the seizure may not be used as evidence of guilt of the suspect or accused person.
2. Persons possessing items or documents to be seized shall not obstruct the officers implementing the seizure. Persons failing to comply with his duty may be fined further to the article 163 of this Code.
3. During seizure the persons specified in the part 4 article 145 of this Code shall be present.
4. If persons possessing the items or documents that must be seized fail to surrender them, the items or documents may be seized with the use of force."

Article 154 of the **CCP** provides coercive investigative measures for real time-control of the content, when pre-trial investigation is started:

"Article 154. Control, Recording and Accumulation of Information Transmitted through Electronic Communications Networks

1. Where there is an order of the judge of pre-trial investigation taken on the grounds of a prosecutor's request, a pre-trial investigation officer may wiretap conversations, transmitted through electronic communications networks, make records, control any other information transmitted through electronic communications networks and make records as well as accumulate if there are grounds to believe that in this way information may be obtained about a **grave crime** or **serious crime** or **less serious crime** either in preparation, in progress or already committed or about **minor crimes** foreseen in Article 170, Article 198(2) Paragraph 1, of the Criminal Code of the Republic of Lithuania, or if there is a danger that violence, coercion or other illegal actions may be used against a victim, witness or other parties to the proceedings or their relatives.

2. The order of the judge of a pre-trial investigation or the decision of a prosecutor to impose wiretapping conversations, transmitting through electronic communications networks, making records, controlling any other information transmitted through electronic communications networks and making records as well as accumulating must specify the following information…

Article 155 of the **CCP** provides investigative measure for collecting any kind of information during pre-trial investigation upon a request of the prosecutor or pre-trial investigation officer:

Article 155. Right of a Prosecutor to Get Familiarised with the Information

1. Having passed a decision and acquired approval of a pre-trial investigation judge a prosecutor has the right to visit any national or municipal, public or private institution, enterprise, or organisation and request to be allowed to get familiarized with the necessary documents or other information, make records or copies of the documents and information, or acquire information in written if this is necessary for investigation of a criminal act.

2. Pursuant to article 163 of this Code a fine can be imposed upon persons refusing to provide information or documents requested by the prosecutor.

3. A prosecutor may use the information acquired in the procedure specified in part 1 of this article only for the purpose of investigation of the criminal act. A prosecutor shall immediately destroy information not necessary for investigation of the criminal act.

4. A pre-trial investigation officer can be commissioned by a prosecutor to get familiarized with the information in the procedure defined by this article.

5. Laws of the Republic of Lithuania can establish limitations on the right of a prosecutor to get familiarized with information."

6.14 Republic of Moldova

Law on preventing and combating cybercrime (No. 20-XVI of 03.02.2009) - The Official Gazette No.11-12/17 of 26.01.2010

Article 7. Obligations of service providers

(1) Service providers are obliged:
a) to keep records of service users;
b) to notify the competent authorities about the web traffic data, including the data about illegal access to computer system information, about the attempts to introduce illegal programs, about the violation by competent persons of the rules of collection, processing, storage, transmission and distribution of information or of rules of computer system protection provided according to the information importance or to its degree of protection, if they have contributed to acquisition, distortion or destruction of information or if they have caused other serious consequences, perturbation of computer systems functioning and other computer crimes;
c) to perform, confidentially, the competent authority's request regarding the immediate preservation of computer data or of web traffic data, which are in danger of destruction or alteration, within 120 calendar days, under the provisions of national legislation;
d) to submit to the competent authorities, on the basis of a request made under the law, the data about users, including the type of communication and the service the user benefited by, the method of payment for the service, as well as about any data that can lead to the identification of the user;
e) to undertake security measures by means of using some procedures, devices or specialized computer programs, with the help of which to restrict or forbid the unauthorized users to access a computer system;
f) to ensure the monitoring, supervision and storage of web traffic data for a period of at least 180 calendar days, in order to identify service providers, service users and the channel by means of which the communication has been transmitted
g) to ensure the interpretation of computer data from network protocols packages, preserving such data for a period of at least 90 calendar days.

(2) If the web traffic data are possessed by several service providers, then the requested service provider is obliged to submit to the competent authority the necessary information for the identification of the other service providers.

Law on preventing and combating cybercrime (No. 20-XVI of 03.02.2009) - The Official Gazette No.11-12/17 of 26.01.2010

Article 10. Requests of competent foreign authorities

(1) Within international cooperation, the competent foreign authority may request that the competent authority from the Republic of Moldova immediately preserve computer data or web traffic data existing in a computer system on the territory of the Republic of Moldova, regarding which the competent foreign authority will submit a well-founded request of international legal assistance in criminal matters.
(2) The request of immediate preservation described in paragraph (1) includes:
a) the name of the authority requesting the preservation;
b) the summary presentation of facts which form the object of prosecution and their legal ratiocination;
c) the computer data which are required to be preserved;
d) any available information necessary for the identification of the computer data owner and the localization of the computer system;

e) the utility of computer data, the necessity of their preservation;
f) the competent foreign authority's intention to submit a request of international legal assistance in criminal matters.
(3) The period of conservation of data recorded in par. (1) shall be not less than 60 calendar days and shall be valid until the competent national authorities decide upon the request of international legal assistance in criminal matters.
(4) Transmission of computer data shall be made only after the acceptance of the request of international legal assistance in criminal matters.

6.15 Norway

Preservation

Criminal Procedure Act section 215a:

"The prosecuting authority may as part of an investigation make an order concerning the securing of electronically stored data deemed to be significant as evidence.

An order concerning the securing of data in a communication that is in the possession of a provider of access to an electronic communications network or electronic communication service may only be made if the conditions in the first paragraph are fulfilled and there is reason to believe that a criminal act has been committed.

The person who is entitled to dispose of the data covered by a security order shall be informed of the order. A suspect shall be informed as soon as the data has been secured and he as been given the status of a suspect. Otherwise information shall be given as soon as the data have been secured.

The security order shall apply for a specific period that must not be longer that necessary and not exceed 90 days at a time. If the security order is made at the request of a foreign State, it shall apply for at least 60 days. Sections 197, third paragraph, 208, first and third paragraphs, and 216 I shall apply correspondingly.

The person who is subject to the order shall on application surrender the traffic data necessary for tracing where the data covered by the security order came from and where they may possibly be sent."

Partial disclosure

For partial disclosure of traffic data, the Norwegian Post and Telecommunications Authority must exempt from the general duty of confidentiality, cf. the Electronic Communication Act Section 2-9 and the Criminal Procedure Act Section 118, first subsection:

"The court may not without the Ministry's consent receive any evidence that the witness cannot give without breaching a statutory duty of secrecy that he has as a consequence of service or work for a family counseling office, a postal agency, a provider of access to an electronic communication network or electronic communication service, electronic communication electrician or the State Airport Company (Avinor). Consent may only be denied if the revelation may be detrimental to the State or public interest or have unfair results for the person who is entitled to the preservation of secrecy.

After giving due consideration to the duty of secrecy, on one hand, and to the clarification of the case, on the other, the court may by order decide that the evidence shall be given even though consent has been denied, or that evidence shall not be received even though the Ministry has consented. Before making such a deciscion, the court shall give the Ministry an opportunity to give an account of the reasons for its point of view. This account shall not be communicated to the parties.

The provision in section 117, second paragraph, shall apply correspondingly."

"The Ministry" mentioned above, is in this case the Post and Telecommunication Authority.

6.16 Portugal

Law no. 109/2009 on Cybercrime of 15 September 2009:

Expedited preservation

Article 12

Expedited preservation of data

1 – If, during the proceedings, when gathering evidence in order to ascertain the truth, it is required to obtain specified computer data stored on a computer system, including traffic data, which might be lost, changed or no longer available, the competent judicial authority orders the person who has the control or availability of such data, including the service provider, to preserve the data in question.
2 - The preservation can also be ordered by the criminal police force, authorized by the judicial authority or even not in emergency or danger in delay but, in this case, notice must be given immediately to the judicial authority, by the report described under Article 253 of the Code of Criminal Procedure.
3 - A preservation order describes, under penalty of nullity:
a) the nature of the data;
b) the origin and destination, if known, and
c) the period of time covered by the preservation order, up to three months.
4 - In compliance with the preservation order addressed to it, whoever has availability or control over such data, including the service provider, preserves immediately the data concerned, protecting and maintaining their integrity for the appointed period of time, in view to allow the competent judicial authority to effectively obtain that information, and remains obliged to ensure the confidentiality of the implementation of these procedures.
5 - The competent judicial authority may order the renewal of the measure for periods of time according to the limit specified in c) of paragraph 3, providing all the requirements, up to a maximum of one year.

Partial disclosure

Article 13

Expedited disclosure of traffic data

In order to ensure the preservation of traffic data from a particular communication, regardless of the number of service providers participating in it, the service provider to whom the preservation has been ordered under the preceding article, discloses to the judicial authority or criminal police force, once known, other service providers through which this communication was carried out in order to identify all service providers used by that communication.

International preservation requests

Article 22

Preservation and expedited disclosure of computer data within international cooperation

1 – Portugal may be requested to expedite preservation of data stored in a computer system located in the country, referring to crimes described under Article 11, in view to submit a request for assistance for search, seizure and disclosure of those data.

2 - The request specifies:
a) the authority requesting the preservation;

b) that the offense is being investigated or prosecuted, as well as a brief statement of the facts relating thereto;
c) the computer data to be retained and its relation to the offense;
d) all the available information to identify the person responsible for the data or the location of the computer system;
e) the necessity of the measure of preservation, and
f) The intention to submit a request for assistance for search, seizure and disclosure of the data.

3 – Executing the demand of a foreign authority under the preceding paragraphs, the competent judicial authority orders the person who has the control or availability of such data, including a service provider, to preserve them.

4 - Preservation can also be ordered by Polícia Judiciária, after authorization obtained from the competent judicial authority or when there is emergency or danger in delay; in this case it is applicable, paragraph 4 of the preceding article.

5 - A preservation order specifies, on penalty of nullity:
a) the nature of the data;
b) if known, the source and their destination, and
c) the period of time during which that data must be preserved for up to three months.

6 - In compliance with the addressed preservation order, who has the control or availability of such data, including a service provider, preserves immediately the data by the specified period of time, protecting and maintaining its integrity.

7 - The competent judicial authority, or Policia Judiciária with permission of the judicial authority, may order the renewal of the measure for periods subject to the limit specified in item c) of paragraph 5, provided they meet the respective requirements of admissibility, to the maximum a year.

8 - When the request referred to in paragraph 1 is received, the competent judicial authority decides the preservation of data until the adoption of a final decision on the request.

9 - Data preserved under this Article may only be provided:
a) to the competent judicial authority, in the execution of the application for cooperation referred to in paragraph 1, in the same way that it could have been done in a similar national case, under Articles 13 to 17;
b) to the national authority which issued the order to preserve, in the same way that it could have been done, in a similar national case under Article 13.

10 - The national authority that, under the preceding paragraph, receives traffic data identifying intermediate service providers by which the communication was made, quickly communicates this fact to the requesting authority in order to enable this authority to submit to the competent authority another request for expedited preservation of data.

11 – The provisions of paragraphs 1 and 2 shall apply, mutatis mutandis, to requests sent to other authorities by the Portuguese authorities.

Article 23 - Grounds for refusal

1 - A request for expedited preservation or disclosure of computer data is refused if:
a) the computer data in question refer to a political offense or a related offense according to Portuguese law;

b) it attempts against the sovereignty, security, ordre publique or other constitutionally defined interests of the Portuguese Republic;
c) the requesting State does not provide guarantees for the protection of personal data.
2 - A request for expedited preservation of computer data can still be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data shall be denied for lack of verification of dual criminality.

6.17 Romania

Expedited preservation and partial disclosure

ART.54 of Romania Law no 161/2003
(1) In urgent and dully justified cases, if there are data or substantiated indications regarding the preparation of or the performance of a criminal offence by means of computer systems, for the purpose of gathering evidence or identifying the doers, the expeditious preservation of the computer data or the data referring to data traffic, subject to the danger of destruction or alteration, can be ordered.
(2) During the criminal investigation, the preservation is ordered by the prosecutor through motivated ordinance, at the request of the criminal investigation body or ex-officio, and during the trial, by the court order.
The measure referred to at paragraph (1) is ordered over a period not longer than 90 days and can be exceeded, only once, by a period not longer than 30 days.
(4) The prosecutor's ordinance or the court order is sent, immediately, to any service provider or any other person possessing the data referred to at paragraph (1), the respective person being obliged to expeditiously preserve them under confidentiality conditions.
(5) In case the data referring to the traffic data is under the possession of several service providers, the service provider referred to at paragraph (4) has the obligation to immediately make available for the criminal investigation body or the court the information necessary to identify the other service providers in order to know all the elements in the communication chain used.
(6) Until the end of the criminal investigation, the prosecutor is obliged to advise, in writing, the persons that are under criminal investigation and the data of whom were preserved.

ART. 55 of Romanian Law 161/2003(in view of making copies that can serve as evidence);
(1) Within the term provided for at art. 54 paragraph (3), the prosecutor, on the basis of the motivated authorisation of the prosecutor specially assigned by the general prosecutor of the office related to the Court of Appeal or, as appropriate, by the general prosecutor of the office related to the Supreme Court, or the court orders on the seizing of the objects containing computer data, traffic data
or data regarding the users, from the person or service provider possessing them, in view of making copies that can serve as evidence.
(2) If the objects containing computer data referring to the data for the legal bodies in order to make copies, the prosecutor mentioned in paragraph (1) or court orders the forced seizure. During the trial, the forced seizure order is communicated to the prosecutor, who takes measures to fulfil it, through the criminal investigation body.
(3) The copies mentioned in paragraph (1) are achieved by the technical means and the proper procedures to provide the integrity of the information contained by them.

International cooperation
Art.63-64 Law no.161/2003
ART.63 of Romania Law no 161/2003
(1) Within the international cooperation, the competent foreign authorities can require from the Service for combating cybercrime the expeditious preservation of the computer data or of the data regarding the traffic data existing within a computer system on the territory of Romania, related to which the foreign authority is to formulate a request of international legal assistance in criminal

matters.
(2) The request for expeditious preservation referred to at paragraph (1) includes the following:
a) the authority requesting the preservation
b) a brief presentation of facts that are subject to the criminal investigation and their legal background;
c) computer data required to be preserved;
d) any available information, necessary for the identification of the owner of the computer data and the location of the computer system;
e) the utility of the computer data and the necessity to preserve them;
f) the intention of the foreign authority to formulate a request of international legal assistance in criminal matters;
(3) The preservation request is executed according to art. 54 for a period of 60 days at the least and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters.

Art.64 of the Law no.161/2003
If, in executing the request formulated according to art.63 paragraph (1), a service provider in another state is found to be in possession of the data regarding the traffic data, the Service for combating cybercrime will immediately inform the requesting foreign authority about this, communicating also all the necessary information for the identification of the respective service provider.

6.18 Serbia

General provisions of article 85 paragraph 1, 146 paragraph 1 and 7, article 155, and 255 paragraph 2, can be applied.

ARTICLE 85
(1) The investigating judge may order on his own initiative or upon the motion of the State Attorney that postal, telephone and other communication agencies retain and deliver to him, against a receipt, letters, telegrams and other shipments addressed to the defendant or sent by him if circumstances exist which indicate that it is likely that these shipments can be used as evidence in the proceedings.
….
amendment 11/9/2009 "Official gazette of Republic Serbia 72/2009"
(4)Measures referred to par 1 of this article shall be reviewed every three months and can last up to nine months. Implementation of measures will be stopped as soon as the reasons for their application are ceased.

6.19 Slovakia

Code of Criminal Procedure
Section 90 of the Code of Criminal Procedure
Preservation and Disclosure of Computer Data

(1) If the preservation of the stored computer data is necessary for the clarification of the facts necessary for the criminal proceedings, including traffic data that is stored through a computer system, the presiding judge and, before the initiation of the criminal prosecution or in the preliminary hearing, the public prosecutor, may issue an order that must be justified even by the merits, to the person who possesses or controls such data, or the provider of such services to

a) store such data and maintain the integrity thereof,

b) allow the production or retention of a copy of such data,

c) render access to such data impossible,

d) remove such data from the computer system,

e) release such data for the purposes of the criminal proceedings.

(2) In the order under Subsection 1 Paragraphs a) or c), a period during which the data storage shall be performed must be determined. This period may be up to 90 days, and if its re-storage is necessary, a new order must be issued.

(3) If the storage of the computer data, including the traffic data for the purpose of the criminal proceedings, is no longer necessary, the presiding judge and, before the onset of the criminal prosecution or in the preliminary hearing, the public prosecutor, shall issue an order for the revocation of the storage of such data without undue delay.

(4) The order under Subsection 1 through 3 shall be served to the person who possesses or controls such data, or to the provider of such services, and they may be imposed an obligation to maintain the confidentiality of the measures specified in the order.

(5) The person who possesses or controls the computer data shall release such data or the provider of services shall issue the information regarding the services that are in their possession or under their control to those who issued the order under Subsection 1 or to the person referred to in the order under Subsection 1.

Section 116 of the Code of Criminal Procedure

(1) In criminal proceedings for an intentional criminal offence, an order for the determination and notification of data on the performed telecommunications operation, which is subject to telecommunications privacy, or subject to personal data protection, which is necessary to clarify the facts relevant to the criminal proceedings, may be issued.

(2) The warrant for the establishment and notification of data on the performed telecommunication operations shall be issued by the presiding judge, before the commencement of the criminal prosecution or in the preliminary hearing upon the petition of the public prosecutor, the judge for preliminary hearing, in writing which must be justified by its merits; the warrant shall be served to the persons referred to in Subsection 3.

Letters Rogatory of Foreign Authorities

Section 537

Method and Form of Letters Rogatory Processing

(1) The Slovak authorities shall perform the legal assistance requested by the foreign authorities in the manner regulated by this Act or an international treaty. If legal assistance is provided under an international treaty in a manner which is not governed by this Act, the competent public prosecutor shall decide in what manner the legal assistance should be performed.

(2) The requested legal assistance may be performed upon the request of a foreign authority under a legal regulation of the requesting State, if the requested procedure is not contrary to the interests protected by the provisions of Section 481.

(3) For the performance of letters rogatory under Section 539 Subsection 1, it is requested that the act, which the letters rogatory concern, is a criminal offence not only under the legal system of the requesting State, but also the legal system of the Slovak Republic.

Section 538

Jurisdiction for the Processing of Letters Rogatory

(1) The letters rogatory of a foreign authority for legal assistance shall be served to the Ministry of Justice.

(2) To ensure the processing of a letter rogatory from a foreign authority for legal assistance, the district prosecution, under which jurisdiction the requested act of legal assistance is to be performed, is competent. If the local jurisdiction is given to several public prosecutions, the Ministry of Justice shall send the letters rogatory to the Attorney General's Office for a decision as to which of the public prosecutions shall provide its processing.

(3) If a foreign authority requests the performance of an interrogation or another act of legal assistance by the court due to the application of the act in the criminal proceedings in the requesting State, the public prosecutor shall submit the letters rogatory of a foreign authority to this extent to the District Court under which jurisdiction the act of legal assistance is to be performed, for processing. If the subject of the letters rogatory is solely an act which is to be performed by the court, the Ministry of Justice shall serve the request directly to the competent court.

Section 539

Permission of an Act of Legal Assistance for the Courts

(1) If the order of the court under this Act is necessary for the performance of evidence requested by a foreign authority, the court shall issue an order upon the petition of the public prosecutor providing the processing of the letters rogatory.

(2) If the act of legal assistance is to be performed under a foreign regulation, the court shall decide, upon the petition of the public prosecutor, whether the procedure under the foreign regulation is not contrary to the interests protected by the provisions of Section 481. If they do not find such conflict, the act shall be permitted and they shall simultaneously decide on the manner of its performance. The public prosecutor may file a complaint against the decision of the court, which has a suspensive effect. The decision of the court on the conflict of the procedure under a foreign regulation shall not be required if it is a serving of documents or instruction of the person under a foreign regulation.

(3) The District Court under which jurisdiction the act of legal assistance is to be performed is competent to make a decision under Subsection 1 and 2.

6.20 Slovenia

Criminal Procedure Law

Article 148
(1) If there are grounds for suspicion that a crime was committed for which the offender is prosecuted ex officio, the police must take steps necessary to trace the offender, that the offender or participant does not hide or flee, to detect and protect the traces of a criminal offense and objects which may be used as evidence and to collect all information that could be useful for the successful conduct of criminal proceedings.

Article 149b
(1) If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed, is being committed or is being prepared or organised, and information on communications using electronic communications networks needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the investigating judge may, at the request of the state prosecutor adducing reasonable grounds, order the operator of the electronic communications network to furnish him with information on the participants in and the circumstances and facts of electronic communications, such as: number or other form of identification of users of electronic communications services; the type, date, time and duration of the call or other form of electronic communications service; the quantity of data transmitted; and the place where the electronic communications service was performed.

(2) The request and order must be in written form and must contain information that allows the means of electronic communication to be identified, an adducement of reasonable grounds, the time period for which the information is required and other important circumstances that dictate use of the measure.

(3) If there are reasonable grounds for suspecting that a criminal offence for which a perpetrator is prosecuted ex officio has been committed or is being prepared, and information on the owner or user of a certain means of electronic communication whose details are not available in the relevant directory, as well as information on the time the means of communication was or is in use, needs to be obtained in order to uncover this criminal offence or the perpetrator thereof, the police may demand that the operator of the electronic communications network furnish it with this information, at its written request and even without the consent of the individual to whom the information refers.

(4) The operator of electronic communications networks may not disclose to its clients or a third party the fact that it has given certain information to an investigating judge (first paragraph of this article) or the police (preceding paragraph), or that it intends to do so.".

Article 150
(1) If there are well-founded grounds for suspecting that a particular person has committed, is committing or is preparing or organising the committing of any of the criminal offences listed in the second paragraph of this Article, and if there exists a well-founded suspicion that such person is using for communications in connection with this criminal offence a particular means of communication or computer system or that such means or system will be used, wherein it is possible to reasonably conclude that other measures will not permit the gathering of data or that the gathering of data could endanger the lives or health of people, the following may be ordered against such person:
1) the monitoring of electronic communications using listening and recording devices and the control and protection of evidence on all forms of communication transmitted over the electronic communications network;
2) control of letters and other parcels;
3) control of the computer systems of banks or other legal entities which perform financial or other commercial activities;

4) wire-tapping and recording of conversations with the permission of at least one person participating in the conversation;

Article 164
(1) The police may even prior to the initiation seize items at 220th of this Act, if it would be dangerous to delay, and the conditions of the 218th of this Act to make home and personal investigation.

Article 220 (seizure of items)
(1) Items which must be take under criminal or may be evidence in criminal proceedings shall be seized and deposited with the court or otherwise protect their storage.

(2) A person who has such items tmust delivered them at the request of the court. If he does not deliver the items, they can to be punished by a fine specified in the first paragraph of Article 78 of this Act, if he still don't want to do, he can be put in prison. Prison lasts until the surrender pf items or until the end of criminal proceedings, but more than one month.

(4) Police officers may seize items mentioned in the first paragraph of this Article, when act in connection with 148t and 164 Article of this Act or when they issuing the court order.

Article 223
(1) The investigating judge may order that the postal, telegraph and other transport organizations and detained against acknowledgment of receipt handed him a letter, telegraph and other items, which are addressed to the defendant or that he sends, if the circumstances, which may cause reasonably be expected to demonstrate in the shipment process.

6.21 "The former Yugoslav Republic of Macedonia"

Criminal Procedure Code (old code)

Temporary securing and seizing of objects or property

Article 203

(1) Objects which according to the Criminal Code are to be seized or may serve as evidence in the criminal procedure, shall be temporarily seized and handed to the court to guard or in another manner secure their guarding.
(2) Whosoever holds such objects shall be obliged to hand them over to the court on its request. The person who refuses to hand over the objects may be punished with a fine determined in Article 74, paragraph 1 of this Code.
(3) The council (Article 22, paragraph 6) shall decide upon an appeal against the determination that imposes a fine. The appeal against the determination shall not withhold the enforcement of the determination.
(4) The authorized officials of the Ministry of Interior can seize the objects listed in paragraph 1 of this Article when they act according to Articles 142 and 147 of this Code or when they execute a court order.
(5) Upon the seizing of the objects the location where they are found shall be notified and described, and if necessary confirmation of their identity shall be provided in another manner. A proof shall be issued for the seized objects.
(6) The confiscated narcotic drugs, psychotropic substances, precursors and other objects prohibited or limited for trade, which are not kept as samples for expertise, by the decision of the competent court, can be destroyed even before the verdict becomes legally valid.

Article 203-a

(1)The investigating judge or the council can, with a determination, stipulate temporary securing of property and means related to the crime. The property and means being subject to securing shall be under court's supervision. Temporary securing of property or objects refers to temporary freezing, confiscation, holding funds, bank accounts and financial transaction or incomes from the crime.
(2)Apart from the objects referred to in Article 203 of this Code, the court can adopt a decision for freezing the means, accounts and funds being suspected to be income from the crime.
(3)The measures for temporary securing of objects, property or means can last until the end of the procedure.
(4)The temporary freezing of accounts can last until the end of the procedure, and its justification shall be re-examined ex officio every two months.
(5)The securing of the immovables shall be done with encumbering a mortgage.
(6)The confiscation of the monetary funds shall be made with an order and they shall be kept in a safety deposit box, or be deposited on a special account without the right to their disposal.
(7)The determination on freezing the financial transaction or bank account shall be submitted to the bank by the court or by other financial institution.
(8)No one can call upon the bank secrecy in order to avoid the enforcement of the court's determination for temporary freezing, confiscation or holding of the funds deposited in the bank.

Article 203-b

A determination for temporary securing of objects or property can be adopted by a court on a request from a foreign state, in the cases anticipated in the international agreements in accordance with the Constitution of the Republic of Macedonia.

Article 203-c

(1)With the determination referred to in Article 203-a of this Code the following cannot be seized:
- the records or other documents of the state bodies which if published could violate the keeping of an official, state or military secrecy, until the competent body decides otherwise;
- the written documents addressed from the defendant to the attorney and the persons referred to in Article 219, paragraph (1) of this Code, unless the defendant hands them in voluntarily;
- technical recordings in possession of the persons referred to in Article 219, paragraph (1) of this Code, made by those persons for facts being released from their duty to testify thereof;
- recordings, excerpts from the register and similar documents in possession of the persons referred to in Article 219, paragraph (1) of this Code, made by them for facts for which they acknowledged from the defendant during their work and
- recordings for facts made by journalists and their editors in mass media from the source of announcement and the information they have acquired during their work and which were used during the editing process of the mass media, which are in their possession or in the redaction where they are employed.

(2)The prohibition of paragraph (1) of this Article shall not apply:
- towards the attorney or the person released from the obligation to testify according to Article 219, paragraph (1) of this Code, if there is a grounded suspicion that they have helped the defendant in committing the crime, or they provided him assistance after the crime was committed or have acted as conceivers or
- if it is a matter of objects which must be seized according to the Criminal Code.

(3)A prohibition for temporary seizing of documents, objects and technical recordings as referred to in paragraph (1) of this Article, shall not apply to crimes regarding damage against children and juveniles. The information kept in devices for automatic i.e. electronic processing of the data and media have to be handed in to the bodies in the criminal procedure in a readable and comprehensible form upon a request of the investigating judge, the council or the sole judge.

Article 203-d

(1)The measures for temporary securing and seizing of objects or property shall be stipulated by a court determination, meaning the investigating judge during the investigation and after initiation of an indictment, the judicial council i.e. a sole judge.

(2)The criminal council, referred to in Article 22 paragraph (6) of this Code, shall decide upon the appeal against the determination of the investigating judge, and the immediate court of higher instance shall decide upon the determination of the trying judge, i.e. of the council.

(3)The objects seized against this Article cannot be used as evidence in the procedure.

Article 204

(1)The state bodies can prohibit showing or issuing of their records or other documents if they consider the issuing of their contents to be harmful to the interests of the state. If the showing or issuing records or other documents is not allowed, the council (Article 22, paragraph 6) shall adopt a final decision.

(2) Legal entities can request the data referring to their work not to be issued.

Article 205

(1) If temporary seizing of records, which may serve as evidence, is performed, such evidence shall be registered. If it is not possible, the records shall be wrapped in a case and shall be sealed. The holder of the records can put his seal on the case.

(2) The person wherefrom the records are seized shall be invited to attend the opening of the case. If he does not reply on the invitation or is absent, the case shall be opened the records shall be inspected and listed in his absence.
(3) During the inspection of the records it must be secured that unauthorized persons would not have access to their contents.

Article 206

(1) The investigating judge can order the legal entities in the field of post, telegraph and other traffic, to keep and, with a confirmation of the receipt, to give to the investigating judge the letters, telegrams and other items addressed to the defendant or sent by the defendant, if there are circumstances according to which it could be expected that these items may serve as evidence in the procedure.
(2) The letters and other parcels shall be opened by the investigating judge in presence of two witnesses. The opening shall be conducted cautiously, in order not to damage the seals, and the case and address shall be kept. Minutes shall be composed for the opening.
(3) If the interests of the procedure allow, the contents of the item can be announced fully or partially to the defendant i.e. the person to whom it is addressed and it may also be handed over to him. If the defendant is absent the item shall be announced or handed over to one of his relatives, and if he has none, it shall be handed to the sender if that does not confront the interests of the procedure.

New Criminal Procedure Law (enters into force in November 2012)

Article 184
Search of a computer system and computer data

(1) Upon request by the person who executes the warrant, the person who uses the computer or has access to it or to another device or data carrier, shall be obliged to provide access to them and give all necessary information required for unobstructed fulfillment of the goals of the search.
(2) Upon request by the person who executes the warrant, the person who uses the computer or has access to it or to another device or data carrier, shall be obliged to immediately take all necessary measures required to prevent the destruction or change of the data.
(3) Any person who uses the computer or has access to it or to another device or data carrier, who fails to proceed pursuant to paragraphs 1 and 2 of this Article, without any justified reasons, shall be punished by the preliminary procedure judge, in accordance with the provisions of Article 88, paragraph 1 of this Law.

6.22 Ukraine

Extract of the new Criminal Procedure Code adopted in April 2012 and entered into force on 19 November 2012:

§ 2. Interference in private communication

Article 258. General provisions related to interference in private communication

1. Nobody may be subjected to interference in private communication without investigating judge's ruling.

2. Public prosecutor, investigator upon approval of public prosecutor shall be required to apply to investigating judge for permission to interfere in private communication as prescribed in Articles 246, 248-250 of the present Code, if any investigative (detective) action implies such interference.

Whenever investigating judge passes the ruling to deny interference in private communication, public prosecutor, investigator may file a new request only with new information.

3. Communication is transmitting information in any way from one person to another directly or using any connection. Communication is considered to be private insofar as information is transmitted and stored under such physical or legal conditions where participants to the communication can expect that such information is protected from interference on the part of others.

4. Interference in private communication implies access to the contents of communication under conditions when participants to the communication can reasonably expect that their communication is private. The following shall be types of interference in private communication:

1) audio, video monitoring of an individual;

2) arrest, examination and seizure of correspondence;

3) collecting information from telecommunication networks;

4) collecting information from electronic information systems.

5. Interference in private communication of defense counsel, between clergyman and the suspect, accused, convict, acquitted shall be forbidden.

Article 259. Preservation of information

1. If public prosecutor intends to use as evidence, during trial, information or any fragment of information obtained as a result of interference in private communication, he shall be required to ensure preservation of all information or delegate preservation of all information to the investigator.

Article 260. Audio, video monitoring of an individual

1. Audio, video monitoring of an individual is a variety of interference in private communication conducted without the individual's knowledge on grounds of a ruling of investigating judge if there are sufficient grounds for the belief that this individual's conversations or other sounds, movements, actions related to his activity or place of stay, etc., can contain information of importance for pre-trial investigation.

Article 261. Arrest of correspondence

1. An individual's correspondence may be arrested without he being aware thereof in exceptional cases based on investigating judge's ruling.

2. Correspondence is arrested if, in the course of pre-trial investigation, there are sufficient grounds for the belief that mail and cable correspondence a certain individual sends to other individuals or is sent from other individuals to the individual concerned, can contain information on circumstances which have importance for pre-trial investigation or objects and documents which have essential importance for pre-trial investigation.

3. Arrest of correspondence entitles the investigator to inspect and seize arrested correspondence.

4. Correspondence referred to in the present Article shall include letters of all types, postal packets, parcels, postal containers, postal money orders, telegrams, and other material mediums for exchange of information among individuals.

5. After the time limit specified in court's ruling has expired, arrest of individual's correspondence is deemed to be revoked.

Article 262. Inspection and seizure of correspondence

1. Seized correspondence shall be inspected in the postal office, which was assigned control and seizure of this correspondence, with participation of this office's representative and, in case of need, of a specialist. In the presence of the said individuals, investigator decides on the opening of correspondence and inspects seized correspondence.

2. Should objects (inclusive of substances), documents be found in the correspondence that are important for a certain pre-trial investigation, investigator within the scope prescribed in the investigating judge's ruling, shall conduct seizure of the correspondence concerned or limit himself to making copies or taking samples of relevant messages. Copies are made or samples taken in view of protecting confidentiality of correspondence arrest. If necessary, the person who inspects mail and cable correspondence, may take a decision to put special marks on the detected objects and documents, equip them with technical control devices, replace objects and substances which endanger surrounding people or are prohibited from being in free circulation, with their safe analogues.

3. If objects or documents of importance for pre-trial investigation are not found in the correspondence, investigator shall give instruction to deliver the correspondence inspected to the addressee.

4. A record shall be drawn up of each occurrence of inspection, seizure or arrest of correspondence as prescribed in the present Code. The record should necessarily state what kind of messages have been inspected, what has been seized from the messages, and what should be delivered to the addressee or temporarily kept, and from what messages copies or samples have been made, and the conduct of other actions as provided for in part two of this Article.

5. Managers and employees of postal offices shall be required to facilitate conducting this covert investigative (detective) action and not to disclose the fact of conducting this covert investigative (detective) action or the information obtained.

Article 263. Collecting information from transport telecommunication networks

1. Collecting information from transport telecommunication networks (networks which provide transmitting of any signs, signals, written texts, images and sounds or messages between telecommunication access networks connected) is a variety of interference in private communication conducted without the knowledge of individuals who use telecommunication facility for transmitting information based on the ruling rendered by the investigating judge, if there is possibility to substantiate the facts during its conducting, which have the importance for criminal proceedings.

2. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics which will allow to uniquely identify the subscriber under surveillance, transport telecommunication network, and terminal equipment which can be used for interference in private communication.

3. Collecting information from transport telecommunication networks means the conducting using appropriate watch facility the surveillance, selection and recording information which is transmitted by an individual and have the importance for pre-trial investigation and also receiving, transformation and recording signals of differebt types which are transmitted by communication channels.

4. Collecting information from transport telecommunication networks is made by responsible units of the bodies of internal affairs and bodies of security. Managers and employees of telecommunication networks' operators shall be required to facilitate conducting the actions on collecting information from transport telecommunication networks, taking required measures in order

not to disclose the fact of conducting such actions and the information obtained, and to preserve it unchanged.

Article 264. Collecting information from electronic information systems

1. Search, detection, and recording information stored in an electronic information system or any part thereof, access to the information system or any part thereof, as well as obtainment of such information without knowledge of its owner, possessor or keeper may be made based on the ruling rendered by the investigating judge, if there is information that such information system or any part thereof contains information of importance for a specific pre-trial investigation.

2. Obtainment of information from electronic information systems or parts thereof the access to which is not restricted by the system's owner, possessor or keeper, or is not related to circumventing a system of logical protection, shall not require permission of investigating judge.

3. Investigating judge's ruling to authorize interference in private communication in such a case should additionally state identification characteristics of the electronic information system which can be used for interference in private communication.

Article 265. Recording and preserving information obtained from communication channels through the use of technological devices and as a result of collecting information from electronic information systems

1. Contents of information which is transmitted by persons via the transport telecommunication networks shall be stated in the record of conducting of the said covert investigative (detective) actions. If such information is found to contain knowledge of importance for a specific pre-trial investigation, the record should reproduce its respective part, and then public prosecutor shall take measures to preserve information obtained by monitoring.

2. Contents of information obtained as a result of monitoring an information system or any part thereof, shall be recorded on the appropriate medium by the individual who has been responsible for monitoring and who is required to ensure processing, preserving, and transmitting the information.

Article 266. Examination of information obtained through the use of technological devices

1. Information obtained through the use of technological devices shall be examined, if necessary, with participation of a specialist. Investigator analyzes contents of the information obtained and draws up a record thereof. In case of detection of information of importance for pre-trial investigation and trial, the record should reproduce the appropriate part of information and then public prosecutor takes measures to preserve information obtained.

2. Technological devices which have been used during the conduct of the said covert investigative (detective) actions, as well as original mediums for received information shall be preserved till the judgment takes legal effect.

3. Mediums and technological devices which helped obtain information may be the subject of examination by appropriate specialists or experts as prescribed in the present Code.

6.23 United Kingdom

Police and Criminal Evidence Act 1984

http://www.legislation.gov.uk/ukpga/1984/60/schedule/1

http://www.homeoffice.gov.uk/publications/police/operational-policing/pace-codes/pace-code-b-2011?view=Binary

Regulation of Investigatory Powers Act (2000)

http://www.legislation.gov.uk/ukpga/1984/60/schedule/1

Acquisition and Disclosure of Communications Data Code of Practice [2007]

Pursuant to section 71 of the Regulation of Investigatory Powers Act 2000
http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary

This Code of Practice provides for access to retained data.

6.24 USA

The U.S. Federal Criminal Code, found at Title 18 of the U.S. Code, includes a provision for data preservation, specifically at U.S. Code, Title 18, Section 2703(f).

The text:

18 U.S.C. § 2703. Required disclosure of customer communications or records.
...
(f) Requirement To Preserve Evidence.—

(1) In general.— A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.— Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

Law enforcement officials obtain partial disclosure of traffic data by issuing a subpoena, as set forth at U.S. Code, Title 18, Section § 2703(c), as follows. Underlined items include the partial disclosure of traffic data.

18 U.S.C. § 2703. Required disclosure of customer communications or records.
...

(c) Records Concerning Electronic Communication Service or Remote Computing Service.
...

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A)name;
(B)address;
(C)local and long distance telephone connection records, or records of session times and durations;
(D)length of service (including start date) and types of service utilized;
(E)telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
(F)means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena... .

7 Appendix 2: Extracts of the Budapest Convention on Cybercrime and explanatory report

7.1 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.

Explanatory report:

Title 2 – Expedited preservation of stored computer data

149. The measures in Articles 16 and 17 apply to stored data that has already been collected and retained by data-holders, such as service providers. They do not apply to the real-time collection and retention of future traffic data or to real-time access to the content of communications. These issues are addressed in Title 5.

150. The measures described in the articles operate only where computer data already exists and is currently being stored. For many reasons, computer data relevant for criminal investigations may not exist or no longer be stored. For example, accurate data may not have been collected and retained, or if collected was not maintained. Data protection laws may have affirmatively required the destruction of important data before anyone realised its significance for criminal proceedings. Sometimes there may be no business reason for the collection and retention of data, such as where customers pay a flat rate for services or the services are free. Article 16 and 17 do not address these problems.

151. "Data preservation" must be distinguished from "data retention". While sharing similar meanings in common language, they have distinctive meanings in relation to computer usage. To preserve data means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. To retain data means to keep data, which is currently being generated, in one's possession into the future. Data retention connotes the accumulation of data in the present and the keeping or possession of it into a future time period. Data

retention is the process of storing data. Data preservation, on the other hand, is the activity that keeps that stored data secure and safe.

152. Articles 16 and 17 refer only to data preservation, and not data retention. They do not mandate the collection and retention of all, or even some, data collected by a service provider or other entity in the course of its activities. The preservation measures apply to computer data that "has been stored by means of a computer system", which presupposes that the data already exists, has already been collected and is stored. Furthermore, as indicated in Article 14, all of the powers and procedures required to be established in Section 2 of the Convention are 'for the purpose of specific criminal investigations or proceedings', which limits the application of the measures to an investigation in a particular case. Additionally, where a Party gives effect to preservation measures by means of an order, this order is in relation to "specified stored computer data in the person's possession or control" (paragraph 2). The articles, therefore, provide only for the power to require preservation of existing stored data, pending subsequent disclosure of the data pursuant to other legal powers, in relation to specific criminal investigations or proceedings.

153. The obligation to ensure preservation of data is not intended to require Parties to restrict the offering or use of services that do not routinely collect and retain certain types of data, such as traffic or subscriber data, as part of their legitimate business practices. Neither does it require them to implement new technical capabilities in order to do so, e.g. to preserve ephemeral data, which may be present on the system for such a brief period that it could not be reasonably preserved in response to a request or an order.

154. Some States have laws that require that certain types of data, such as personal data, held by particular types of holders must not be retained and must be deleted if there is no longer a business purpose for the retention of the data. In the European Union, the general principle is implemented by Directive 95/46/EC and, in the particular context of the telecommunications sector, Directive 97/66/EC. These directives establish the obligation to delete data as soon as its storage is no longer necessary. However, member States may adopt legislation to provide for exemptions when necessary for the purpose of the prevention, investigation or prosecution of criminal offences. These directives do not prevent member States of the European Union from establishing powers and procedures under their domestic law to preserve specified data for specific investigations.

155. Data preservation is for most countries an entirely new legal power or procedure in domestic law. It is an important new investigative tool in addressing computer and computer-related crime, especially crimes committed through the Internet. First, because of the volatility of computer data, the data is easily subject to manipulation or change. Thus, valuable evidence of a crime can be easily lost through careless handling and storage practices, intentional manipulation or deletion designed to destroy evidence or routine deletion of data that is no longer required to be retained. One method of preserving its integrity is for competent authorities to search or similarly access and seize or similarly secure the data. However, where the custodian of the data is trustworthy, such as a reputable business, the integrity of the data can be secured more quickly by means of an order to preserve the data. For legitimate businesses, a preservation order may also be less disruptive to its normal activities and reputation than the execution of a search and seizure of its premises. Second, computer and computer-related crimes are committed to a great extent as a result of the transmission of communications through the computer system. These communications may contain illegal content, such as child pornography, computer viruses or other instructions that cause interference with data or the proper functioning of the computer system, or evidence of the commission of other crimes, such as drug trafficking or fraud. Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required (see further explanation on the importance of traffic data below under Article 17). Third, where these

communications contain illegal content or evidence of criminal activity and copies of such communications are retained by service providers, such as e-mail, the preservation of these communications is important in order to ensure that critical evidence is not lost. Obtaining copies of these past communications (e.g., stored e-mail that has been sent or received) can reveal evidence of criminality.

156. The power of expedited preservation of computer data is intended to address these problems. Parties are therefore required to introduce a power to order the preservation of specified computer data as a provisional measure, whereby data will be preserved for a period of time as long as necessary, up to a maximum of 90 days. A Party may provide for subsequent renewal of the order. This does not mean that the data is disclosed to law enforcement authorities at the time of preservation. For this to happen, an additional measure of disclosure or a search has to be ordered. With respect to disclosure to law enforcement of preserved data, see paragraphs 152 and 160.

157. It is also important that preservation measures exists at the national level in order to enable Parties to assist one another at the international level with expedited preservation of stored data located in their territory. This will help to ensure that critical data is not lost during often time-consuming traditional mutual legal assistance procedures that enable the requested Party to actually obtain the data and disclose it to the requesting Party.

Expedited preservation of stored computer data (Article 16)

158. Article 16 aims at ensuring that national competent authorities are able to order or similarly obtain the expedited preservation of specified stored computer-data in connection with a specific criminal investigation or proceeding.

159. 'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. It requires that it be kept safe from modification, deterioration or deletion. Preservation does not necessarily mean that the data be 'frozen' (i.e. rendered inaccessible) and that it, or copies thereof, cannot be used by legitimate users. The person to whom the order is addressed may, depending on the exact specifications of the order, still access the data. The article does not specify how data should be preserved. It is left to each Party to determine the appropriate manner of preservation and whether, in some appropriate cases, preservation of the data should also entail its 'freezing'.

160. The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor). In some States, preservation orders do not exist in their procedural law, and data can only be preserved and obtained through search and seizure or production order. Flexibility is intended by the use of the phrase 'or otherwise obtain' to permit these States to implement this article by the use of these means. However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases.

161. The power to order or similarly obtain the expeditious preservation of specified computer data applies to any type of stored computer data. This can include any type of data that is specified in the order to be preserved. It can include, for example, business, health, personal or other records. The measures are to be established by Parties for use "in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification." This can include situations where the data is subject to a short period of retention, such as where there is a business policy to delete the data after a certain period of time or the data is ordinarily deleted when the storage

medium is used to record other data. It can also refer to the nature of the custodian of the data or the insecure manner in which the data is stored. However, if the custodian were untrustworthy, it would be more secure to effect preservation by means of search and seizure, rather than by means of an order that could be disobeyed. A specific reference to "traffic data" is made in paragraph 1 in order to signal the provisions particular applicability to this type of data, which if collected and retained by a service provider, is usually held for only a short period of time. The reference to "traffic data" also provides a link between the measures in Article 16 and 17.

162. Paragraph 2 specifies that where a Party gives effect to preservation by means of an order, the order to preserve is in relation to "specified stored computer data in the person's possession or control". Thus, the stored data may actually be in the possession of the person or it may be stored elsewhere but subject to the control of this person. The person who receives the order is obliged "to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure." The domestic law of a Party should specify a maximum period of time for which data, subject to an order, must be preserved, and the order should specify the exact period of time that the specified data is to be preserved. The period of time should be as long as necessary, up to a maximum of 90 days, to permit the competent authorities to undertake other legal measures, such as search and seizure, or similar access or securing, or the issuance of a production order, to obtain the disclosure of the data. A Party may provide for subsequent renewal of the production order. In this context, reference should be made to Article 29, which concerns a mutual assistance request to obtain the expeditious preservation of data stored by means of a computer system. That article specifies that preservation effected in response to a mutual assistance request "shall be for a period not less than 60 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."

163. Paragraph 3 imposes an obligation of confidentiality regarding the undertaking of preservation procedures on the custodian of the data to be preserved, or on the person ordered to preserve the data, for a period of time as established in domestic law. This requires Parties to introduce confidentiality measures in respect of expedited preservation of stored data, and a time limit in respect of the period of confidentiality. This measure accommodates the needs of law enforcement so that the suspect of the investigation is not made aware of the investigation, as well as the right of individuals to privacy. For law enforcement authorities, the expedited preservation of data forms part of initial investigations and, therefore, covertness may be important at this stage. Preservation is a preliminary measure pending the taking of other legal measures to obtain the data or its disclosure. Confidentiality is required in order that other persons do not attempt to tamper with or delete the data. For the person to whom the order is addressed, the data subject or other persons who may be mentioned or identified in the data, there is a clear time limit to the length of the measure. The dual obligations to keep the data safe and secure and to maintain confidentiality of the fact that the preservation measure has been undertaken helps to protect the privacy of the data subject or other persons who may be mentioned or identified in that data.

164. In addition to the limitations set out above, the powers and procedures referred to in Article 16 are also subject to the conditions and safeguards provided in Articles 14 and 15.

7.2 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.

Explanatory report:

Expedited preservation and partial disclosure of traffic data (Article 17)

165. This article establishes specific obligations in relation to the preservation of traffic data under Article 16 and provides for expeditious disclosure of some traffic data so as to identify that other service providers were involved in the transmission of specified communications. "Traffic data" is defined in Article 1.

166. Obtaining stored traffic data that is associated with past communications may be critical in determining the source or destination of a past communication, which is crucial to identifying the persons who, for example, have distributed child pornography, distributed fraudulent misrepresentations as part of a fraudulent scheme, distributed computer viruses, attempted or successfully accessed illegally computer systems, or transmitted communications to a computer system that have interfered either with data in the system or with the proper functioning of the system. However, this data is frequently stored for only short periods of time, as laws designed to protect privacy may prohibit or market forces may discourage the long-term storage of such data. Therefore, it is important that preservation measures be undertaken to secure the integrity of this data (see discussion related to preservation, above).

167. Often more than one service provider may be involved in the transmission of a communication. Each service provider may possess some traffic data related to the transmission of the specified communication, which either has been generated and retained by that service provider in relation to the passage of the communication through its system or has been provided from other service providers. Sometimes traffic data, or at least some types of traffic data, are shared among the service providers involved in the transmission of the communication for commercial, security, or technical purposes. In such a case, any one of the service providers may possess the crucial traffic data that is needed to determine the source or destination of the communication. Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination.

168. Article 17 ensures that where one or more service providers were involved in the transmission of a communication, expeditious preservation of traffic data can be effected among all of the service

providers. The article does not specify the means by which this may be achieved, leaving it to domestic law to determine a means that is consistent with its legal and economic system. One means to achieve expeditious preservation would be for competent authorities to serve expeditiously a separate preservation order on each service provider. Nevertheless, obtaining a series of separate orders can be unduly time consuming. A preferred alternative could be to obtain a single order, the scope of which however would apply to all service providers that were identified subsequently as being involved in the transmission of the specific communication. This comprehensive order could be served sequentially on each service provider identified. Other possible alternatives could involve the participation of service providers. For example, requiring a service provider that was served with an order to notify the next service provider in the chain of the existence and terms of the preservation order. This notice could, depending on domestic law, have the effect of either permitting the other service provider to preserve voluntarily the relevant traffic data, despite any obligations to delete it, or mandating the preservation of the relevant traffic data. The second service provider could similarly notify the next service provider in the chain.

169. As traffic data is not disclosed to law enforcement authorities upon service of a preservation order to a service provider (but only obtained or disclosed subsequently upon the taking of other legal measures), these authorities will not know whether the service provider possesses all of the crucial traffic data or whether there were other service providers involved in the chain of transmitting the communication. Therefore, this article requires that the service provider, which receives a preservation order or similar measure, disclose expeditiously to the competent authorities, or other designated person, a sufficient amount of traffic data to enable the competent authorities to identify any other service providers and the path through which the communication was transmitted. The competent authorities should specify clearly the type of traffic data that is required to be disclosed. Receipt of this information would enable the competent authorities to determine whether to take preservation measures with respect to the other service providers. In this way, the investigating authorities can trace the communication back to its origin, or forward to its destination, and identify the perpetrator or perpetrators of the specific crime being investigated. The measures in this article are also subject to the limitations, conditions and safeguards provided in Articles 14 and 15.

7.3 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.

Explanatory report:

Expedited preservation of stored computer data (Article 29)

282. This article provides for a mechanism at the international level equivalent to that provided for in Article 16 for use at the domestic level. Paragraph 1 of this Article authorises a Party to make a request for, and paragraph 3 requires each Party to have the legal ability to obtain, the expeditious preservation of data stored in the territory of the requested Party by means of a computer system, in order that the data not be altered, removed or deleted during the period of time required to prepare, transmit and execute a request for mutual assistance to obtain the data. Preservation is a limited, provisional measure intended to take place much more rapidly than the execution of a traditional mutual assistance. As has been previously discussed, computer data is highly volatile. With a few keystrokes, or by operation of automatic programs, it may be deleted, altered or moved, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. Thus, it was agreed that a mechanism was required in order to ensure the availability of such data pending the lengthier and more involved process of executing a formal mutual assistance request, which may take weeks or months.

283. While much more rapid than ordinary mutual assistance practice, this measure is at the same time less intrusive. The mutual assistance officials of the requested Party are not required to obtain possession of the data from its custodian. The preferred procedure is for the requested Party to ensure that the custodian (frequently a service provider or other third party) preserve (i.e., not delete) the data pending the issuance of process requiring it to be turned over to law enforcement officials at a later stage. This procedure has the advantage of being both rapid and protective of the privacy of the person whom the data concerns, as it will not be disclosed to or examined by any government official until the criteria for full disclosure pursuant to normal mutual assistance regimes have been fulfilled. At the same time, a requested Party is permitted to use other procedures for ensuring the rapid preservation of data, including the expedited issuance and execution of a production order or search warrant for the data. The key requirement is to have an extremely rapid process in place to prevent the data from being irretrievably lost.

284. Paragraph 2 sets forth the contents of a request for preservation pursuant to this Article. Bearing in mind that this is a provisional measure and that a request will need to be prepared and transmitted rapidly, the information provided will be summary and include only the minimum information required to enable preservation of the data. In addition to specifying the authority that is seeking preservation and the offence for which the measure is sought, the request must provide a summary of the facts, information sufficient to identify the data to be preserved and its location, and a showing that the data is relevant to the investigation or prosecution of the offence concerned and that preservation is necessary. Finally, the requesting Party must undertake to subsequently submit a request for mutual assistance so that it may obtain production of the data.

285. Paragraph 3 sets forth the principle that dual criminality shall not be required as a condition to providing preservation. In general, application of the principle of dual criminality is counterproductive in the context of preservation. First, as a matter of modern mutual assistance practice, there is a trend to eliminate the dual criminality requirement for all but the most intrusive procedural measures,

such as search and seizure or interception. Preservation as foreseen by the drafters, however, is not particularly intrusive, since the custodian merely maintains possession of data lawfully in its possession, and the data is not disclosed to or examined by officials of the requested Party until after execution of a formal mutual assistance request seeking disclosure of the data. Second, as a practical matter, it often takes so long to provide the clarifications necessary to conclusively establish the existence of dual criminality that the data would be deleted, removed or altered in the meantime. For example, at the early stages of an investigation, the requesting Party may be aware that there has been an intrusion into a computer in its territory, but may not until later have a good understanding of the nature and extent of damage. If the requested Party were to delay preserving traffic data that would trace the source of the intrusion pending conclusive establishment of dual criminality, the critical data would often be routinely deleted by service providers holding it for only hours or days after the transmission has been made. Even if thereafter the requesting Party were able to establish dual criminality, the crucial traffic data could not be recovered and the perpetrator of the crime would never be identified.

286. Accordingly, the general rule is that Parties must dispense with any dual criminality requirement for the purpose of preservation. However, a limited reservation is available under paragraph 4. If a Party requires dual criminality as a condition for responding to a request for mutual assistance for production of the data, and if it has reason to believe that, at the time of disclosure, dual criminality will not be satisfied, it may reserve the right to require dual criminality as a precondition to preservation. With respect to offences established in accordance with Articles 2 through 11, it is assumed that the condition of dual criminality is automatically met between the Parties, subject to any reservations they may have entered to these offences where permitted by the Convention. Therefore, Parties may impose this requirement only in relation to offences other than those defined in the Convention.

287. Otherwise, under paragraph 5, the requested Party may only refuse a request for preservation where its execution will prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. Due to the centrality of this measure to the effective investigation and prosecution of computer- or computer-related crime, it was agreed that the assertion of any other basis for refusing a request for preservation is precluded.

288. At times, the requested Party will realise that the custodian of the data is likely to take action that will threaten the confidentiality of, or otherwise prejudice, the requesting Party's investigation (for example, where the data to be preserved is held by a service provider controlled by a criminal group, or by the target of the investigation himself). In such situations, under paragraph 6, the requesting Party must be notified promptly, so that it may assess whether to take the risk posed by carrying through with the request for preservation, or to seek a more intrusive but safer form of mutual assistance, such as production or search and seizure.

289. Finally, paragraph 7 obliges each Party to ensure that data preserved pursuant to this Article will be held for at least 60 days pending receipt of a formal mutual assistance request seeking the disclosure of the data, and continue to be held following receipt of the request.

7.4 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.

Explanatory report:

Expedited disclosure of preserved traffic data (Article 30)

290. This article provides the international equivalent of the power established for domestic use in Article 17. Frequently, at the request of a Party in which a crime was committed, a requested Party will preserve traffic data regarding a transmission that has travelled through its computers, in order to trace the transmission to its source and identify the perpetrator of the crime, or locate critical evidence. In doing so, the requested Party may discover that the traffic data found in its territory reveals that the transmission had been routed from a service provider in a third State, or from a provider in the requesting State itself. In such cases, the requested Party must expeditiously provide to the requesting Party a sufficient amount of the traffic data to enable identification of the service provider in, and path of the communication from, the other State. If the transmission came from a third State, this information will enable the requesting Party to make a request for preservation and expedited mutual assistance to that other State in order to trace the transmission to its ultimate source. If the transmission had looped back to the requesting Party, it will be able to obtain preservation and disclosure of further traffic data through domestic processes.

291. Under Paragraph 2, the requested Party may only refuse to disclose the traffic data, where disclosure is likely to prejudice its sovereignty, security, *ordre public* or other essential interests, or where it considers the offence to be a political offence or an offence connected with a political offence. As in Article 29 (Expedited preservation of stored computer data), because this type of information is so crucial to identification of those who have committed crimes within the scope of this Convention or locating of critical evidence, grounds for refusal are to be strictly limited, and it was agreed that the assertion of any other basis for refusing assistance is precluded.