COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/TCY

Strasbourg, version 21 June 2015 T-CY (2015)7

## Cybercrime Convention Committee (T-CY)

# Assessment report

# Implementation of the preservation provisions of the Budapest Convention on Cybercrime

# Follow up given by Parties

**Adopted by the 13th Plenary of the T-CY (15-16 June 2015)**

**Contents**



**Contact**


Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY) Tel +33-3-9021-4506
Directorate General of Human Rights and Rule of Law Fax +33-3-9021-5650
Council of Europe, Strasbourg, France Email: alexander.seger@coe.int

# 1 Background

The T-CY at its 8th Plenary (December 2012) adopted the Assessment Report on the implementation of the expedited preservation provisions of the Budapest Convention on Cybercrime. The report foresaw as follow up that:

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

The 11th T-CY Plenary discussed the matter in June 2014 and decided:

> To invite Parties to submit information in writing to the Secretariat by 31 August 2014 on follow up given to the Assessment Report adopted in December 2012 (T-CY(2012)10rev) where domestic provisions were considered "partially" or "not in line" with the Budapest Convention – and other Parties to submit additional information as appropriate – in view of the preparation of a draft report for consideration by the 12th Plenary;

The 12th T-CY Plenary (2-3 December 2014) decided:

> Agenda item 5: Follow up to T-CY Assessment Report on the expedited preservation provisions
>
> - To note that the additional replies to the questionnaire and the information provided by Parties on follow up given to the T-CY assessment report on expedited preservation and the impact of the data retention ruling of the European Court of Justice did not allow the T-CY Bureau to prepare a supplementary report as decided by the 11th Plenary;
> - To request the Secretariat to invite Parties concerned to provide additional information with a deadline for replies of 20 January 2015;
> - To invite the Bureau to submit a supplementary report on expedited preservation for consideration by the 13th Plenary of the T-CY (June 2015);

In 2012, 31 Parties participated in the assessment of the expedited preservation provisions.

In June 2014 and again in December 2014,

- Parties concerned were invited to provide information on follow up given with respect to provisions where they were partially or not in line with the Budapest Convention. Parties were also invited to provide information in cases where legislative developments since December 2012 have led to lesser consistency with the Budapest Convention.
- All Parties were invited to provide a brief update on data retention regimes, including in the light of the judgment of the European Court of Justice.[1]

The present report summarises information received and provides a brief assessment of follow up given to the 2012 report by Parties.

The report was adopted by T-CY 13 (15-16 June 2015).

---

[1] http://curia.europa.eu/juris/document/document.jsf?text=Data%2BRetention&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=305870#ctx1

**Summary of results of the 2012 assessment**

| **Party**<br>(Y = in line<br>P = Partially in line<br>N = Not in line with the Budapest Convention) | **Article 16 Expedited preservation in 2012** | **Article 29 Expedited preservation (international) in 2012** | **Article 17 Preservation and partial disclosure in 2012** | **Article 30 Preservation and partial disclosure (international) in 2012** |
|---|---|---|---|---|
| 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. Estonia | P | P | P | P |
| 9. Finland | Y | Y | Y | Y |
| 10. France | Y | Y | Y | Y |
| 11. Georgia | P | P | P | P |
| 12. Germany | Y | Y | P | P |
| 13. Hungary | Y | P | P | N |
| 14. Italy | Y | | Y | Y |
| 15. Latvia | Y | Y | Y | Y |
| 16. Lithuania | P | P | P | P |
| 17. Republic of Moldova | P | Y | Y | Y |
| 18. Montenegro | Y | Y | P | P |
| 19. Netherlands | Y | Y | Y | Y |
| 20. Norway | Y | Y | Y | Y |
| 21. Portugal | Y | Y | Y | Y |
| 22. Romania | Y | Y | Y | Y |
| 23. Serbia | Y | Y | Y | Y |
| 24. Slovakia | Y | Y | No information | No information |
| 25. Slovenia | P | P | P | P |
| 26. Spain | N | N | N | N |
| 27. Switzerland | Y | Y | Y | No information |
| 28. "The former Yugoslav Republic of Macedonia" | Y | Y | P | P |
| 29. Ukraine | N | N | N | N |
| 30. United Kingdom | Y | Y | Y | Y |
| 31. United States of America | Y | Y | Y | P |

## 2 Follow up given by Parties to the assessment report 2012[2]

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| 1. Albania | Y | Y | Y | Y | ✓ |
| 2. Armenia | N | N | N | N | Information provided<br><br>On 24.08.2012 by order of the Prosecutor General an interdepartmental working group was established in order to prepare amendments to the Criminal Code and Criminal Procedure Code of the RA. The working group comprised representatives from the Prosecutors General's office, Police and National Security Service. OSCE office in Yerevan supported the interdepartmental working group and the Council of Europe supported a study visit to Portugal.<br><br>The working group has prepared:<br>– Draft amendments to Criminal Procedure Code of the RA to ensure compliance of internal legislation with articles 16, 17, 29, 30 of the Convention on Cybercrime which was sent to the working group preparing a new CPC of the Republic of Armenia.<br>– Draft amendments to the Criminal Code to ensure compliance of Chapter 24 and Articles 144, 178, 181, 263 Criminal Code with Articles 2 to 9 of Convention on Cybercrime, which later on was sent by the Ministry of Justice to the working group on the Criminal Code for consideration.<br><br>So far, despite the steps undertaken, the national legislation does not yet |

[2] Table based on Page 79 of the Assessment Report (document T-CY(2012)10).
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)10_Assess_report_v31_public.pdf

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | comply with the Convention on Cybercrime, including Articles 16, 17, 29, 30 Convention on Cybercrime.<br>According to the authorities of Armenia, it is difficult to predict the timeline for adoption of the new Criminal Code and Criminal Procedure Code. Until that time, domestic legislation of the Republic of Armenia is not in line with the Convention on Cybercrime.<br><br>T-CY assessment<br><br>Armenia ratified the Budapest Convention in 2006, but domestic legislation is still not in line with the Convention. Reforms have been underway for several years.<br>The T-CY requests the authorities of Armenia to complete the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime without further delays. |
| 3. Azerbaijan | P | P | Y | Y | Information provided<br><br>No additional developments.<br><br>T-CY assessment<br><br>The T-CY requests the authorities of Azerbaijan to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime. |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| 4. Bosnia and Herzegovina | P | P | P | P | Information provided<br><br>The authorities of Bosnia and Herzegovina communicated a number of amendments dealing with channels of communication, MLA requests in urgent cases, grounds for refusal and joint investigative teams (see appendix).<br><br>However, the amendments communicated seem not to fill the gaps identified in the Assessment Report (2012) on preservation of computer data.<br><br>Additional amendments are planned for 2015 to bring domestic legislation in line with the Convention.<br><br>T-CY assessment<br><br>The T-CY requests the authorities of Bosnia and Herzegovina to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime. |
| 5. Bulgaria | Y | Y | Y | Y | ✓ |
| 6. Croatia | Y | Y | Y | Y | ✓ |
| 7. Cyprus | P | P | P | N | Information provided<br><br>No additional information received to permit a follow-up in line with the Rules of Procedures. |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | T-CY assessment<br><br>The T-CY request the authorities of Cyprus to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime. |
| 8. Estonia | P | P | P | P | Information provided<br><br>Estonia is starting a comprehensive review of the whole Criminal Procedure Code in 2015. During the review, legislation concerning the electronic evidence, including the collection and preservation of data will also be examined. The review will be followed by legislative amendments.<br><br>T-CY assessment<br><br>The T-CY requests the authorities of Estonia to complete the necessary reforms to bring domestic regulations and practices fully in line with the Budapest Convention on Cybercrime. |
| 9. Finland | Y | Y | Y | Y | ✓ |
| 10. France | Y | Y | Y | Y | ✓ |
| 11. Georgia | P | P | P | P | Information provided<br><br>At the domestic level, production orders are used to order the preservation of data. |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | Under the Law on international law enforcement cooperation, adopted in October 2013 with additional amendments to this law in February 2015, a request under Article 29 received within the framework of the Budapest Convention can be executed. Partial disclosure in line with Article 30 is also possible.<br><br>Proposals for additional amendments to procedural law are before Parliament based on which secondary regulations will be enacted in line with the Budapest Convention.<br><br>T-CY assessment<br><br>Georgia appears now in line with Article 16, 17, 29 and 30. |
| 12. Germany | Y | Y | P | P | Information provided<br><br>Germany and the T-CY Bureau had extensive exchanges with regard to Article 29 (see appendix).<br><br>T-CY assessment<br><br>The additional clarifications provided by the authorities of Germany seem to support the T-CY assessment of 2012.<br><br>With regard to Article 29, the T-CY may review the functioning in practice again at a later stage based on further experience by Parties. |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | With regard to Articles 17 and 30, T-CY requests the authorities of Germany to consider the necessary legislative reforms and undertake additional measures to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime. |
| 13. Hungary | Y | P | P | N | Information provided<br><br>No additional information received to permit a follow-up in line with the Rules of Procedures.<br><br>T-CY assessment<br><br>The T-CY requests the authorities of Hungary to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime. |
| 14. Italy | Y | - | Y | Y | Information provided<br><br>Regarding Articles 16 and 17, Italy uses search and seizure orders according to the Italian Criminal Procedure Code.<br><br>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 |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | data), 248 (production orders), 254 (seizure of correspondence), 259 (custody of things seized, including of data preserved), 352 (searches, including technical measures to preserve data), and 354 (urgent investigations and seizure, including securing of data and computer systems).<br><br>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 (except for traffic data held by service providers).<br><br>For traffic data from service providers, Italy uses the special provisions of section 132 of Personal Data Protection Code for preservation of traffic data from providers. The preservation order can be issued in relation to any crime.<br><br>With regard to international requests under Articles 29 and 30, in principle, an MLA request is required. Italian authorities can use information provided by a foreign authority via law enforcement channels (such as Interpol or Europol) or via 24/7 point of contact or via Eurojust to open a case in Italy in order to use a search and seizure order issued by the public prosecutor to preserve electronic evidence (see above).<br><br>Traffic data may also be preserved following a request from a foreign investigating authority under Section 132 paragraph 4-ter of the Personal Data Protection Code.<br>For handing over the data (retained/preserved) to a foreign authority, an MLA request is required |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | See the Appendix for additional information provided.<br><br>T-CY assessment<br><br>Italy is in line with Articles 16 and 17, and partially in line with 29 and 30 of the Convention.<br><br>The T-CY requests the authorities of Italy to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime. |
| 15. Latvia | Y | Y | Y | Y | ✓ |
| 16. Lithuania | P | P | P | P | Information provided:<br><br>The authorities of Lithuania provided the following explanations:<br><br>Article 16 – Expedited preservation of stored computer data<br><br>Art 65 Para 2 of the LEC sets out an obligation to public communication network and (or) service providers to preserve and disclose, in accordance with the procedures established by the law and for the purposes of prevention, disclosure and investigation of criminal offences, to competent authorities the data generated and processed by them. |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | Article 17 – Expedited preservation and partial disclosure<br><br>Based on Art 77 Para 1 of the LEC, economic entities providing electronic communication networks and (or) services, shall, in accordance with the procedures established by the law, disclose immediately the information that is available to them and which is necessary to prevent, investigate and detect criminal offences, to the requesting competent authorities (criminal intelligence, pre-trial investigation entities, public prosecutors, judges) on the basis of their request.<br><br>Art 29 – Expedited Preservation of Stored Computer Data (international), Art 30 – Expedited Disclosure of Preserved Traffic Data<br><br>Upon receipt of a request from a foreign point of contact, The Cybercrime Board (24/7 Contact Point) has the right to send out lawful requests to Lithuanian entities to preserve data available to them and obtain data and other information disclosure of which does not require court rulings (basic subscriber information, partially traffic data). Should data or other information the disclosure of which requires court ruling be needed, an MLAT procedure should be applied.<br><br>Expedited data preservation tool as provided in Art 29 of the Budapest Convention is effectively used in Lithuania as both the requested and the requesting party. In average, 20-30 preservation requests from other states |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | are processed and 10-15 sent to foreign countries annually by Cybercrime Board. Main countries for cooperation: Belarus, Germany, Latvia, Moldova, the Netherlands, Romania, Ukraine, United Kingdom, USA.<br><br>T-CY assessment<br><br>Lithuania is in line with Articles 16, 17, 29 and 30. |
| 17. Republic of Moldova | P | Y | Y | Y | Information provided<br><br>Article 4 of the Law on Preventing and Combating Cybercrime (Law nr. 20-XVI of 03/02/2009) determines the functions of public authorities and institutions responsible for preventing and combating cybercrime. The General Prosecutor's Office can order the immediate preservation of computer data if there is danger of destruction or alteration in accordance with the law of criminal procedure. The request is issued by a prosecutor.<br><br>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.<br><br>A court order is required for the subsequent production of data.<br>This measure is often used and considered essential for investigations.<br><br>With respect to Article 29, Moldova has specific provisions that cover |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | preservation of computer data. The order is enforceable against any person.<br><br>T-CY assessment:<br><br>Moldova uses a combination of special provisions for preservation along with general powers. The Republic of Moldova is now in line with Article 16, 17, 29 and 30. |
| 18. Montenegro | Y | Y | P | P | Information provided<br><br>No additional developments.<br><br>T-CY assessment:<br><br>The T-CY requests the authorities of Montenegro to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime. |
| 19. Netherlands | Y | Y | Y | Y | ✓ |
| 20. Norway | Y | Y | Y | Y | ✓ |
| 21. Portugal | Y | Y | Y | Y | ✓ |
| 22. Romania | Y | Y | Y | Y | Information provided<br><br>Romania enacted a new Criminal Procedure Code on 1 February 2014. Most of the previous provisions regarding preservation of the previous law |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | implementing the Budapest Convention have been maintained. However, the preservation provisions (Article 154 CPC and Article 64 of Law 161/2003) are now limited to service providers.<br><br>Current specific provisions in combination with general powers such as search, seizure (Article 168 CPC) and production orders (Article 152 CPC) still permit the preservation of data with regard to any person.<br><br>For international requests (Article 29 and 30) the provisions of the previous law 161/2003 are still applied, however, limited to service providers.<br>Amendments are before Parliament to remove this lacuna.<br><br><u>T-CY assessment</u><br><br>The T-CY requests the authorities of Romania to undertake the necessary reforms to bring domestic regulations and practices again in line with the Budapest Convention on Cybercrime. |
| 23. Serbia | Y | Y | Y | Y | <u>Information provided</u><br><br>The envisaged changes of Criminal Procedural Code in 2015 will more precisely implement the provisions of the Budapest Convention in order to achieve more consistent implementation, including with respect to the execution of MLA requests.<br><br>The current articles of the Criminal Procedural Code together with provisions of |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | the Law on Mutual Legal Assistance in Criminal Matter do allow actions provided by said CETS Articles but with implementation of various other procedural tools at disposal to the Police, Prosecution or Courts.<br><br>T-CY assessment<br><br>The T-CY encourages the authorities of Serbia to complete the necessary reforms in view of specific preservation provisions in line with the Budapest Convention on Cybercrime. |
| 24. Slovakia | Y | Y | No inform-ation | No information | Information provided<br><br>The relevant provisions are contained in Sections 69, 69a to 69g of the Chapter Four (Processing information by the Police Corps) and Sections 72 to 77c Chapter Six (Relations of the Police Corps to the national authorities, municipalities, legal and natural persons and abroad) of the Act No. 171/1993 Coll. on the Police Corps as amended.<br><br>As regards the EU and EEA countries, the expedited disclosure of preserved traffic data is assured be means of Europol-SIENA. Other countries are covered by the bilateral agreements concluded by Slovakia which are, in general, the Council of Europe Member States which ratified/acceded to the Budapest Convention. Until now, the competent national authorities do not record any serious problems. Even the current Draft Regulation and the preceding Council Decision are regulating the possibility of providing information to third countries on the basis of the agreements with Europol, when there is a security risk. As |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | for criminal proceedings, the situation is similar and assured by means of EUROJUST and also relevant bilateral agreements concluded by Slovakia. As regards the Slovak Police Corps, the exchange and expedited disclosure of preserved traffic data is done on the basis of Act No. 171/1993 Coll. on the Police Corps as amended in compliance with the Act No. 122/2013 Coll. on Personal Data Protection.<br><br>T-CY assessment<br><br>Regarding Articles 17 and 30 is partially in line with the Convention.<br><br>The T-CY encourages the authorities of Slovakia to complete the necessary reforms in view of specific preservation provisions in line with the Budapest Convention on Cybercrime. |
| 25. Slovenia | P | P | P | P | Information provided<br><br>The Ministry of Justice proposed some changes in Criminal Procedure Code in article 149//b in order to facilitate a better implementation of expedited preservation provisions. The proposal is still in parliamentary procedure.<br><br>In the meantime the Slovenian authorities had two requests from other parties/EU members for expedited preservation that have been solved successfully.<br><br>T-CY assessment |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | The T-CY requests the authorities of Slovenia to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime, including through specific preservation provisions covering all types of data and all kinds of holders of data. |
| 26. Spain | N | N | N | N | Information provided<br><br>Reforms are underway, a Draft Bill amending the Criminal Procedural Law, wich will include preservation provisions, is currently being under parliamentary scrutiny and most likely will be passed in the second semester of 2015.<br><br>T-CY assessment:<br><br>Spain has no special provision for preservation or partial disclosure as per Article 16 and 17 Budapest Convention.<br>However, national legislation covers a large range of provisions that enable Spain to secure data without delay, including provisions for search and seizure of information system/computer data (Spanish Code of Criminal Procedure Articles 567 et seq.); or production orders may be used for obtain electronic evidence in a swift manner. The judicial authority can access subscriber information, in any event, in the course of a criminal investigation, in accordance with Article 18 of the Spanish Constitution and specific rules.<br>In Spain, both the Constitutional Court and the Supreme Court have traditionally held that when access to information does not affect the confidentiality of a communication but merely the right to personal privacy, and |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | circumstances of urgency and necessity exist, access to such information would be possible in the exercise of the legitimate duties of law enforcement for the prevention and investigation of an offence, discovery of criminals and gathering the instruments, effects and evidence thereof — on the basis of Articles 282 of the Code of Criminal Procedure, Article 11(1) of Framework Law 2/1986 of 13 March 1986 on the law enforcement agencies and Article 14 of Framework Law 1/1992 of 21 February 1992 on the protection of the safety of citizens.<br>Also in Spain, the data retention law introduced special provisions and procedures with respect to access and use of the retained traffic data (Law 25/2007 of 18 October 2007).<br><br>As for art. 29 and art. 30 Budapest Convention, Spain seems to be partially in line since data can be obtained (including disclosure) directly by other means then preservation. Some of the national instruments used for, requires mutual legal assistance request.<br><br>The reform of the Criminal Procedural Code currently in the Parliament includes introduction of special provision regarding preservation of data with Article 588 (j), and by this Spain will have additional tools that can be used both at the national and international level.<br><br>The T-CY requests the authorities of Spain to complete the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime, including through specific preservation provisions. |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | |
| 27. Switzerland | Y | Y | Y | No information | Information provided<br><br>In order to comply with Article 30 of the Convention, Switzerland has introduced, in 2012, a new provision into its *Federal Act on International Mutual Assistance in Criminal Matters*. Article 18b reads as follows:<br><br>Art. 18*b*[1] Electronic communications traffic data<br><br>1 The federal or cantonal authority dealing with a request for mutual assistance may order the transmission of electronic communications traffic data to another State before conclusion of the mutual assistance proceedings if:<br>a. provisional measures indicate that the communication that is the subject of the request originated abroad; or<br>b. the data was acquired by the executing authority based on an order for authorised real-time surveillance (Art. 269–281 of the CrimPC[2]).<br><br>2 The data may not be used in evidence before the ruling on granting and the extent of mutual assistance is legally binding.<br><br>3 Notice of the ruling under paragraph 1 and any order or authorisation for surveillance must be given to the Federal Office immediately.<br><br>According to this additional provision, the transmission of traffic data to the requesting State can be ordered and executed in an expedited manner, before |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | formally concluding the mutual assistance proceedings.<br><br>Traffic data are provided, according to article 18b, alternatively in cases where indications show that the subject of the request is located abroad (for example in a third country) or where such information was acquired during a real-time-surveillance.<br><br>Such expedited disclosure of traffic data can only be performed in the understanding that the data sets are to be used in order to promote and facilitate criminal investigations in the requesting State. The data can be used as evidence in a (foreign) court only after the Swiss MLA proceedings have been authorised or approved by a national court's ruling (in case the measures were contested).<br><br>From a practical point of view, the number of requests for such expedited disclosures has been quite low, in the first 3 years after the entry into force of the provision (probably less than 10; no official statistics available). A raising number of States Parties to the Convention and an enhanced exchange of information may also lead to a rise of such cases in the near future<br><br><u>T-CY assessment:</u><br><br>The T-CY is of the opinion that on the basis of the information provided Switzerland is in line with Article 30. |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | |
| 28. "The former Yugoslav Republic of Macedonia" | Y | Y | P | P | <u>Information provided</u><br><br>The new CPC (Official gazette 150/2010) has new articles regarding Articles 17 and Article 30 of the Convention, namely, Articles 184, 198, 252 paragraphs 1, 4, 5 and 6. In addition, the Law for international cooperation in criminal matters (Official gazette 124/2010) includes relevant articles, that is, Articles 15, 25 and 29.<br><br>The authorities use general powers (search, seizure, production order) in order to preserve data.<br><br>Regarding the implementation of article 30, the domestic legislation states that:<br>"(1) Domestic judicial authority at the request of a foreign competent authority take temporary measures to collect evidence and ensuring evidence already collected or for the protection of threatened legal interests.<br>(2) Acting under the MLA request of paragraph (1) of this Article a domestic judicial authority may act or partial execution, or the executing of the MLA request can be time limited"(Article 29 of the Law for international cooperation in criminal matters)<br><br><u>T-CY assessment</u><br><br>Article 29 of the Law for international cooperation in criminal matters |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | (temporary measures) requires an MLA request. This is not in line with Article 29 Budapest Convention.<br><br>With regard to Article 17 Budapest Convention the above provisions may be sufficient. With regard the international partial disclosure (Article 30 Budapest Convention), "The former Yugoslav Republic of Macedonia" appears not to be in line as an MLA request is required.<br><br>The T-CY requests the authorities of "The former Yugoslav Republic of Macedonia" to undertake the necessary reforms to bring domestic regulations and practices in line with Articles 29 and 30 Budapest Convention. |
| 29. Ukraine | N | N | N | N | <u>Information provided</u><br><br>Authorities (including Ukrainian Ministry of Interior (MVD) and Security Service of Ukraine (SSU)), participating in the intergovernmental working task group have prepared a consolidated draft Law on Cyber Security of Ukraine which is to be submitted to the Cabinet of Ministries for confirmation (attached).<br>Also the Ministry of justice of Ukraine was notified of the need to incorporate into the Criminal Procedures Code of Ukraine provisions on expedited preservation and other powers required in the Budapest Convention.<br><br>It is hoped that legislative changes be adopted before the new Ukrainian Parliament will be elected, thus, by 26 October 2015.<br><br>Ukraine would also like to remind the T-CY that procedures on data |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | preservation and expedited data preservation on international requests as well are observed in the Criminal Procedures Code of Ukraine in the frame of the MLAT mechanism. In other words, preservation and disclosure of data on the requests of international law enforcement authorities are followed when the MLA request mentioning that is received by the General Prosecutors Office of Ukraine. That office then issues an order to the specific law-enforcement body of Ukraine to fulfill the MLAT. The law-enforcement basing on the order of the GPO office receive court order and go to the ISP in order to obtain the necessary data.<br><br>T-CY assessment<br><br>The T-CY requests the authorities of Ukraine to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime, including through specific preservation provisions. |
| 30. United Kingdom | Y | Y | Y | Y | ✓ |
| 31. United States of America | Y | Y | Y | P | Information provided<br><br>There are no new developments.<br><br>T-CY assessment<br><br>The T-CY requests the authorities of the USA to undertake the necessary reforms to bring domestic regulations and practices in line with Article 30 Budapest Convention. |

| | Results of assessments in 2012 | | | | Update 2015 on follow up given by Parties |
|---|---|---|---|---|---|
| **Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)** | **Article 16 Expedited preserv.** | **Article 29 Expedited preserv. (inter-national)** | **Article 17 Preserv. and partial disclosure** | **Article 30 Preserv. and partial disclosure (internation.)** | **Follow up given by Parties or relevant developments and T-CY Assessment** |
| | | | | | |

# 3 Update on data retention regulations

**All Parties** have been invited to provide a brief update on data retention regimes, including in the light of the judgment of the European Court of Justice.[3]

| Party | Information provided in 2012[4] | Update (situation as at May 2015) |
|---|---|---|
| 1. Albania | Yes, 2 years | No change. |
| 2. Armenia | No | Under consideration 6-12 months. |
| 3. Australia | | A new data retention regime will enter into force in October 2015. Retention period will be 2 years. |
| 4. Austria | | Data retention law declared unconstitutional in July 2014. |
| 5. Azerbaijan | No (under consideration) | Still under consideration. |
| 6. Belgium | | Belgium had legislation on data retention since the Bill of 30 July 2013 and the Royal Decree of 19 September 2013. The retention period was one year.<br>On 11 June 2015, the Constitutional Court annulled the data retention law. |
| 7. Bosnia and Herzegovina | Yes, 1 year | This matter is regulated by the Decision of Council of Ministers of Bosnia and Herzegovina on specific obligations of legal and natural persons providing telecommunication services, managing telecommunication networks and performing telecommunication activities, regarding security and maintenance of capacities which enable authorized agencies to perform legal interception of telecommunications, as well as telecommunication data protection and security capacities (Official Gazette of Bosnia and Herzegovina, No. 104/06, 58/07). Articles 23. – 29. of the Decision stipulate retention of stored computer data for the period of 12 months |
| 8. Bulgaria | Yes, 1 year. Data accessed may be retained a further 6 months | Recent change: duration of retention reduced to 6 months. |
| 9. Croatia | Yes, 1 year | No change |
| 10. Cyprus | Yes, 6 months | |
| 11. Czech Republic | | 6 months data retention.<br><br>Section 97 para. 3 of the Act No. 127/2015 on electronic communications stipulates as follows:<br><br>"Natural or legal person providing public communications |

[3] http://curia.europa.eu/juris/document/document.jsf?text=Data%2BRetention&docid=150642&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=305870#ctx1

[4] Page 74 of document T-CY(2012)10 http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)10_Assess_report_v31_public.pdf

| Party | Information provided in 2012[4] | Update (situation as at May 2015) |
|---|---|---|
| | | network or providing publicly available electronic communications services is obliged to store **for 6 months traffic and location data**, which are produced or processed when providing public communications network and when providing their publicly available electronic communications services. After period of 6 months data must be destroyed. The obliged person must secure that content of such data will not be stored and forwarded. Law enforcement authorities have to first obtain a court warrant in order to access these data."<br>This provision means that the **traffic and location data** are automatically (without the need of any request) stored by obliged persons for period of 6 months. The law enforcement authorities can be given access to them if the statutory conditions are fulfilled, this applies regardless of whether one or more service providers were involved (every provider must store traffic and location data). |
| 12. Denmark | Yes, 1 year | The information on data retention regulation is still valid |
| 13. Dominican Republic | | 3 months data retention |
| 14. Estonia | Yes, 1 year | In May 2014 Ministry of Justice, together with the Ministry of Interior and Ministry of Economic Affairs and Communications started an analysis in order to examine legislation implementing the Data Retention Directive, in particular Criminal Procedure Code and Electronic Communications Act.<br>The analysis hasn't been finalised yet.<br>In February 2015, the Constitutional Court decided that data retention rules in Estonia were in line with the Constitution. |
| 15. Finland | Yes, 1 year | Previously, as mentioned in page 74 of the attached adopted assessment report on preservation (or page 6 in doc. T-CY (2014)23), the retention period has been 1 year. After the total reform of our information society legislation and starting from the 1.1.2015 the new retention periods are more fine tuned, after the preliminary assessment of the decision of the ECJ. In short it can be said that retention periods are:<br>- 1 year for mobile telephone services<br>- 9 months for internet connection services<br>- 6 months for internet telephone service. |
| 16. France | Yes, 1 year | No impact following the judgment of the European Court of Justice. The French law on data retention is prior to the EU directive. |
| 17. Georgia | Yes, 2 years | On 30 November 2014, the Parliament of Georgia adopted a package of legal amendments to various acts, aimed at reform of covert police operations involving telephone wiretapping and interception of traffic and content data. As a part of the reform, Article $8^3$ has been introduced to the |

| Party | Information provided in 2012[4] | Update (situation as at May 2015) |
|---|---|---|
| | | Law on Electronic Communications of Georgia, which entitles law enforcement authorities to access ISP infrastructure directly and copy and retain all traffic data for 2 years (unofficial translation of this provision attached as a separate document). However, there are ongoing discussions as to constitutionality (right to privacy) and proportionality (in light of 2014 European Court of Justice decision on Data Retention Directive) of the retention practice and revision is expected before the end of the year. |
| 18. Germany | | At present, under German law there is no mandatory data retention. However, according to § 96 Telecommunication Act (TKG) providers may store data for the purposes laid down in the TKG (for example for billing purposes). That means, that data are stored for at least a couple of days .<br><br>On 27 May 2015, German Federal Government adopted a draft law on mandatory data retention. The draft law provides for the mandatory retention of traffic data for a period of ten weeks and of location data for a period of four weeks. Law enforcement authorities may obtain retained data if:<br><br>1. facts give rise to the suspicion that a person has committed one of several listed particularly serious criminal offences,<br>2. the offence is particularly serious in the individual case as well,<br>3. other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success and<br>4. access to the data is proportionate.<br><br>By combining a relatively short period of retention with a reduction of the categories of data to be retained and strict access regulation, the planned date retention regime complies with the standards laid down by the European Court of Justice in its judgment of 8 April 2014 (C-293/12 and C-594/12). |
| 19. Hungary | Yes, 6 months for unsuccessful calls, 1 year for other data | |
| 20. Iceland | | The Data Retention Directive 2006/24/EC was never implemented into Icelandic law. However the Icelandic Electronic Communications Act pertains similar rules on data retention and has since 2005.<br>Data retention is therefore allowed and the rules have not been changed despite the ruling of the ECJ of April 8, 2014. The reason for that is that the Icelandic version is considered somewhat more proportionate than the EU |

| Party | Information provided in 2012[4] | Update (situation as at May 2015) |
|---|---|---|
| | | Directive. Data should only be retained for 6 months, and must be disposed of after that time limit. Moreover the data cannot be accessed under any circumstance unless authorities have first obtained a court ruling to that regard. In addition the legislation stipulates certain security requirements for all telecom operators.<br>It is nevertheless foreseeable that the rules will have to be reviewed in due course. |
| 21. Italy | Yes, 24 months for telephony data, unsuccessful calls 30 days, 12 months for Internet data | The information on data retention regulation is still valid as the judgment of the European Court of Justice did not have influence on the Italian personal data protection code (Legislative Decree no.196 of 30 June 2003).<br><br>Art. 4-bis of the Law n. 43 of 17 April 2015 provides that, in order to implement the investigation regarding only serious crimes indicated in art. 51.3-quater and 407.3.a) of Italian criminal procedure code, traffic data (except for contents data) must be retained by the Internet service providers and operators until 31 December 2016**.** |
| 22. Japan | | No data retention.<br>Japan does not have data retention. Based on the "Cyber Security Strategy" which is a Japan's national cyber security policy which was adopted in June 2013, Japan has been discussing the way of the preservation of traffic data by relevant ISPs in order to ensure the possibility to track cybercrime after the incident. |
| 23. Latvia | Yes, 18 months | No change. |
| 24. Lithuania | Yes, 6 months | Entities that provide public communication networks and (or) services are obliged under the Law on Electronic Communications of the Republic of Lithuania to preserve certain categories of data that are necessary for the prevention, disclosure and investigation of criminal offences for a period of 6 months. On a lawful request of competent authorities (criminal intelligence, pre-trial investigation entities), this period may be prolonged for another 6 months. After the preservation period, data must be destroyed. |
| 25. Luxembourg | | |
| 26. Malta | | 6 months for internet data and telephone data for 1 year. |
| 27. Mauritius | | 3 months data retention as per Directive of ICT authority. Specific legislation in preparation. |
| 28. Republic of Moldova | Yes, 3 months | |
| 29. Montenegro | Yes | 6 to 24 months. |
| 30. Netherlands | Yes, 1 year | Service providers are required to retain traffic data / subscriber info for telecommunications for 12 months and for internet communications for 6 months. With the proper investigation powers law enforcement can order disclosure |

| Party | Information provided in 2012[4] | Update (situation as at May 2015) |
|---|---|---|
| | | of such data.<br>Consultations have started on a newly proposed bill on data retention that will respect the current required periods for retention, but will limit the disclosure of telecommunication data. Only in situations where there is suspicion of a crime carrying a maximum of at least eight years' imprisonment the law enforcement agencies may order full disclosure of data for the whole period of 12 months. Otherwise the LEA's can only ask disclosure of data from the last 6 months. For internet communications data can be ordered 6 months back.<br>On November 17, 2014, Dutch cabinet send a letter to Parliament in which the cabinet reacted on the ruling of the Court of Justice of 8 April 2014. First of all the cabinet stipulates the ECJ ruling does not annul the Dutch law on data retention. The cabinet also underlines the need for data retention, especially in relation to the investigation into and prosecution of serious crime. Giving up data retention will seriously hamper the law enforcement response to inter alia frauds, armed robbery, murder, child pornography, and, terrorism and jihadism. Dutch government reminds Parliament that also the ECJ itself declared that there may be added value in keeping data. In conclusion the cabinet sticks to the current requirement to retain traffic data / subscriber info for telecommunications for 12 months and for internet communications for 6 months.<br>Nevertheless, Dutch cabinet issued also a draft bill on data retention. This draft does not propose to change the time periods for retention. They will remain at 12 months for telecommunications and 6 months for internet communications. The draft does propose to change the disclosure of kept data. Only in situations where there is suspicion of a crime carrying a maximum of at least eight years' imprisonment the law enforcement agencies may order full disclosure of data for the whole period of 12 months. Otherwise the LEA's can only ask disclosure of data from the last 6 months. For internet communications data can be ordered 6 months back. Furthermore disclosure will require not only an order by a prosecutor, but also the approval of a judge.<br>On March 11 2015, the Hague District Court suspended the law on data retention. The court concluded that that current law violates citizen's fundamental rights to respect for private life and to the protection of personal data. The ministry is studying the judgment and is contemplating a possible appeal.<br>Meanwhile the ministry states that work is done to swiftly bring to parliament a bill for a new data retention regime. Meanwhile the Dutch Code of criminal procedure still |

| Party | Information provided in 2012[4] | Update (situation as at May 2015) |
|---|---|---|
| | | contains the provisions on disclosure of data residing with ISP's. ISP's do retain records on communications of customers for their own administrative procedures, in a period from one month onward to a specified date , and in practice on average for 6 months. As long as the company possesses these data, the providers are obliged to cooperate with justice. But they are not obliged anymore to retain records 12 months, and they are not obliged to retain specific types of data that are relevant for prosecution purposes. |
| 31. Norway | No | No obligatory data retention. The issue is under review. Currently, ISPs may store internet traffic data for up to 21 days, according to the Norwegian Data Protection Authority's interpretation of the Personal Data Act Article 28 (cf. EU Directive 95/46/EC Article 6 nr. 1 e). |
| 32. Panama | | |
| 33. Poland | | 12 months data retention. |
| 34. Portugal | Yes, 1 year | The previous regulation (Law 32/2008) is still formally in force.<br>It is generally understood that the national law, that provides a wide range of safeguards (regarding retention and storage of data, access to data, monitoring and assessment of the retention among other), fulfils the essential requirements of the ECJ ruling. Thus, as by May 2015, no initiative was developed, in view of revising the law.<br>Also by May 2015, there are no records of any court decision regarding the validity of the law.<br>Besides, the ISP keep retaining data and providing them to LEA, according to that law. |
| 35. Romania | No | The Constitutional Court on 8 July 2014 (decision 440) declared the law on data retention unconstitutional.<br>Many investigations stopped since. |
| 36. Serbia | Yes, 12 months | No change but court order required to access data. |
| 37. Slovakia | Yes, 1 year fixed and mobile telephony data, 6 months for Internet access, email and telephony data | On 23 April 2014 the Constitutional Court suspended data retention provisions. |
| 38. Slovenia | Yes, 14 months telephony data, 8 months Internet-related data | In July 2014, the Constitutional Court repealed the section in our Electronic Communication Act regarding data retention. They lean their decision on the EU Court which had repealed the EU Data Retention Directive. Thus, all Internet and mobile providers/operators were required to erase all data. Now they can only store data for their billing needs - this sort of data is usually stored for a period of up to three month (but this period also differs among |

| Party | Information provided in 2012[4] | Update (situation as at May 2015) |
|---|---|---|
| | | operators/providers). Before they were obliged to store data for 12 months (data for fixed and mobile phone services) and for 8 months (data for Internet services)."<br><br>Update: A working group was formed to fill the legal gap that now exists in data retention law, i.e. our electronic communication law. Right now they are some proposals for provisions that the data would be stored for 3 months. Also there are proposals that a judge, police or public prosecutor could order ISP to preserve data for 3 months with an option for additional 3 months (according to articles 16 and 29 of CCC). But right now it's too soon to say what will be the outcome. |
| 39. Spain | Yes, 1 year | The Data Retention Directive, 2006/24/CE, was transposed into national legislation by Law 25/2007 of October 18. This Domestic Data Retention Law is currently valid and enforceable; and its compliance with constitutional standards has not been challenged until now. |
| 40. Switzerland | Yes, 6 months | Swiss Parliament is currently revising national legislation on the surveillance of communications. According to the current draft, while being aware of the judgement of the European Court of Justice, the mandatory data retention time period will be prolonged from 6 months to 12 months (see article 273 para. 3 of the amended Swiss Procedural Code: https://www.admin.ch/opc/fr/federal-gazette/2013/2483.pdf). The legislative amendments are assumed to enter into force in 2016. |
| 41. "The former Yugoslav Republic of Macedonia" | Yes | No change. |
| 42. Turkey | | Data retention 12 months. |
| 43. Ukraine | Yes, 3 years | No change. |
| 44. United Kingdom | Yes, 1 year | New data retention regime. |
| 45. United States of America | No | No new developments. |

# 4 T-CY conclusions

## 4.1 Overall conclusions regarding preservation provisions

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. Preservation measures are particularly important at a time when procedural law powers and regulations on data retention are uncertain and where questions arise regarding jurisdiction in the context of cloud computing.

2. As already noted in the assessment of 31 Parties in 2012, the assessment of additional States shows that "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 ….. 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."

3. The T-CY, therefore, underlines the recommendations already made in 2012:

   - 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.

   - Parties that are not able to preserve or otherwise secure electronic evidence in an expedited manner and do therefore not comply with the relevant Articles of the Budapest Convention, are encouraged to take urgent steps to enable their competent authorities to preserve electronic evidence in domestic and international proceedings.

## 4.2 Conclusions regarding follow up given to the 2012 assessment

The T-CY,

4. Expresses its thanks to the Parties which provided additional information on follow up given to the 2012 assessments;

5. Welcomes the reforms undertaken in Georgia which brought domestic legislation in line with the preservation provisions of the Budapest Convention;

6. Notes that reforms are underway in Armenia, Estonia, Romania, Serbia, Slovenia and Ukraine, and requests Parties to ensure that the reforms are completed in due course and bring domestic legislation in line with the preservation provisions of the Budapest Convention;

7. Requests other Parties which are not or only partially in line with one or more of the preservation articles to undertake the necessary reforms to bring domestic regulations and practices in line with Articles16, 17, 29 and 30 Budapest Convention;

8. Regrets that several Parties did not provide information to permit follow up to the previous assessment in line with the Rules of Procedures, and requests the Chair of the T-CY to address specific letters to the authorities of these Parties to recall the need for cooperation in the assessments carried out by the Cybercrime Convention Committee.

### 4.3 Follow up

9. The T-CY invites all Parties to provide a further update regarding the functioning of preservation provisions and reforms undertaken by December 2016.

# 5 Appendix: Additional information provided by Parties

## 5.1 Bosnia and Herzegovina

The Bosnia and Herzegovina authorities replied:

Ministry of Justice of Bosnia and Herzegovina emphasized amendments to the Law on Mutual Legal Assistance in Criminal Matters (The Official Gazzette of Bosnia and Herzegovina, no. 58/13) in terms of development of the international cooperation, referring also to Art. 29. And 30. of the Convention on Cybercrime.

Relevant provisions have been amended as follows:

**"Article 4**
**Channels of Communication**

(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.
"(4 In urgent cases, requests for mutual legal assistance may be forwarded and received through Eurojust – the European Union Agency for police and judicial cooperation in criminal matters.
(5) Procedure of competent bodies of Bosnia and Herzegovina in relations with Eurojust, shall be regulated by specific instruction of Miniser of Justice of Bosnia and Herzegovina, by which institutions and contact point for cooperation with Europol will be appointed.
(6) In cases of communication referred to in Paragraphs (2) and (3) of this Article, the national judicial authority shall communicate a copy of the request for mutual legal assistance to the Ministry of Justice of Bosnia and Herzegovina.
(7) The Ministry of Justice of Bosnia and Herzegovina shall transmit and receive through the Ministry of Foreign Affairs of Bosnia and Herzegovina the requests for mutual legal assistance to/from a foreign State that has no international treaty in force with Bosnia and Herzegovina, as well as in cases when an international treaty explicitly envisages use of diplomatic channels of communication.
(8) 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.
Upon receipt of a request from a foreign 24/7 contact point, which contains all the necessary data, the same is delivered to competent BiH police bodies for further proceedings.

**Article 5**
**Urgency of Proceeding**

(1) The Ministry of Justice of Bosnia and Herzegovina shall transmit, without delay, request for mutual assistance by a foreign judicial authority to the relevant nationaljudicial authority for further action, unless it is evident that the request is not in compliance with an international treaty and this Law, in which case it should be refused.
(2) The Ministry of Justice of Bosnia and Herzegovina shall also act promptly upon requests for mutual legal assistance of the national judicial authorities, unless it is evident that the request is not in compliance with an international treaty and that a foreign authority would refuse it. In such a case, the request shall be returned to the national judicial authority in order to eliminate failures."
Current paragraph (2), which becomes paragraph (3), shall be amended to read as follows:
"(3) In cases referred to in Article 4 paragraph (3) of this Law, the authority of Bosnia and Herzegovina which is competent for cooperation with Interpol shall communicate the request directly to the competent national judicial authority, wherein it shall be obliged to communicate a

copy of the request and the referral document to the Ministry of Justice of Bosnia and Herzegovina."

**Article 9**

**(Grounds for Denying Mutual Assistance)**

"(1) Apart from other reasons for denying requests for certain forms of legal assistance as foreseen by this Law, a relevant national judicial authority shall deny a request for legal assistance in the following cases:

(a) if the execution of the request would prejudice the legal order of Bosnia and Herzegovina or its sovereignty or security;

(b) if the request concerns an offence which is considered to be a political criminal offence or an offence connected with a political criminal offence;

(c) if the request concerns a military criminal offence;

d) if the person to whom the request pertains has been acquitted of charges based on the substantive-legal grounds or if the proceeding against him has been discontinued, or if he was relieved of punishment, or if the sanction has been executed or may not be executed under the law of the State where the verdict has been passed;

e) if criminal proceedings are pending against the accused in Bosnia and Herzegovina for the same criminal offence, unless the execution of the request might lead to a decision releasing the accused from custody;

(a) if criminal prosecution or execution of a sanction pursuant to the national law would be barred by the statute of limitations.

(2) The provisions of paragraph (1), sub-paragraph d) of this Article shall not apply in cases of reopening the criminal proceedings in the requesting State.

(3) In addition to the reasons as stipulated in paragraph (1) of this Article, legal assistance may also be denied on the basis of actual reciprocity with a certain State."

**Article 10**

**(Exemptions from Denying Legal Assistance)**

(1) Crimes against humanity or other values protected by international law may not serve as a basis to deny the request for mutual legal assistance in terms of Article 9, sub-paragraphs b) and c) of this Law.

(3) No request for mutual legal assistance shall be denied solely because it concerns an offence which is considered to be a fiscal offence pursuant to national law.

**Article 24**

**(Joint Investigation Teams)**

(1) If the circumstances of the specific case so justify, joint investigation teams may be formed by an agreement between the relevant Prosecutor's Office in Bosnia and Herzegovina and the relevant authorities of a foreign State for the purpose of conducting the criminal investigation on the territory of one or more contracting states which have formed a joint team for a restricted period of time.

(2) The agreement shall define: the composition of the team, the tasks of the team, its authority and the period of time to which it has been formed. If so agreed by the signatory parties to the agreement, the team may extend its operation even after expiry of the deadline set forth in the agreement.

(3) A request for setting a joint team should include data as referred to in Article 3 of this Law, and it may be filed by any interested party. The request shall be filed through the Ministry of Justice of Bosnia and Herzegovina to the relevant Prosecutor's Office in Bosnia and Herzegovina, along with the proposal for the team composition. In the same manner, a Prosecutor with the relevant Prosecutor's Office in Bosnia and Herzegovina shall forward such request to the relevant judicial authority of the foreign State, if he finds it necessary.

(4) The team shall be formed in one of the signatory parties to the agreement in which the investigative actions are expected to be taken. The request shall also include a proposal for the team composition.

(5) A joint investigation team may be formed when:

a) investigation of criminal offences conducted in one State requires a complex and thorough investigation connected with other States;

b) several parties conduct investigation of criminal offences whose nature requires coordinated and harmonised actions by the States involved;

c) investigative actions should be taken in turn in Bosnia and Herzegovina and in another State, that is, in several States.

(6) A joint investigation team shall act on the territory of Bosnia and Herzegovina under the following conditions:

a) the Team Leader shall be a Prosecutor with the relevant Prosecutor's Office in Bosnia and Herzegovina;

b) the team shall take investigative actions in accordance with the criminal legislation in Bosnia and Herzegovina, and national and foreign members of the joint team shall perform their tasks lead by the Teal Leader;

c) the relevant Prosecutor's Office in Bosnia and Herzegovina shall take all required organisational measures to meet the needs of the team.

(7) Foreign members of the joint investigation team shall have the right to stay on the territory of Bosnia and Herzegovina during the investigation. For certain reasons and in compliance with the legislation of Bosnia and Herzegovina, the Team Leader may decide otherwise.

(8) The Team Leader may transfer powers to foreign members of the joint investigation team for taking certain investigative actions in accordance with the legislation of Bosnia and Herzegovina and with the consent of the relevant foreign judicial authorities of the State foreign members came from.

(9) If a joint investigation team is to take investigative actions on the territory of Bosnia and Herzegovina, national members of the team may ask the relevant authorities in Bosnia and Herzegovina to take such actions. These actions shall be taken in compliance with laws of Bosnia and Herzegovina.

(10) If, during an investigation on the territory of Bosnia and Herzegovina, the joint investigation team requires a legal assistance from a third State, a request for mutual legal assistance shall be filed by a relevant national judicial authority.

(11) The relevant national judicial authorities may use information the national or foreign members reached in the course of their work in the joint investigation team, which is not available otherwise, for the following purposes:

a) for the purpose for which the team has been established;

b) for detection, investigation or prosecution of other criminal offences, with the consent of the State to whose foreign members information has been made available;

c) for prevention of direct or serious threat to public safety and without prejudice to the provisions of sub-paragraph b) if the criminal investigation is to be instigated at a later point in time;

d) for other purposes if so agreed upon by the parties which have formed the team."

## 5.2 Germany

**Information provided on 12 September 2014 by the Federal Ministry of Justice on follow up given**

Germany has adopted a new law that explicitly allows the identification of the holder of a dynamic IP address. § 100j (new) of the criminal code of procedure requires the provider of telecommunication services to immediately give information on stored computer data (such as the the holder of dynamic ip address). To obtain the data, a court decision is required. In urgent cases however, the public prosecutor or even the police can order to release the data.

Above that, Germany has thoroughly considered the content of the assessment report, especially the assessment of Germany's traffic data provisions. German law provides for the temporary freezing of traffic data and also allows law enforcement authorities to obtain the data directly (§ 100g of the Criminal Code of procedure). Germany considers traffic data as especially sensitive. The release of traffic data can infringe the fundamental rights of citizens. Therefore, the principle of proportionality requires the legislation to obtain the limitations.

**Comment by the USA dated 23 December 2014 regarding the information provided by Germany**

The US has one comment. Unfortunately, the US cannot agree that Germany complies with the convention with respect to preservation for foreign requests.
Our understanding, based on practical experience, is that Germany carries out a search or obtains a production order when another country requests preservation. The requesting country must submit sufficient facts to a prosecutor for evaluation. If the prosecutor is not satisfied with the submission, the search or production order is not approved. The prosecutor may ask the requesting country for additional facts. There is no provision for special speed due to the perishability of electronic evidence. Nor is the process simple. Searches and production orders apparently must wait either until formal mutual legal assistance has been submitted or until a formal mutual assistance request has been promised. In every case, immediately or later, preservation in Germany requires a formal mutual legal assistance request.
Thus, in the practical experience of the US, a lot of work must be done by both countries *merely to ensure that data is not destroyed*. This situation does not accord with the aim of the convention to streamline and speed preservation. (This is particularly problematic because Germany has no data retention and observes data destruction.) The procedures of most other Parties are noticeably more helpful.
For these reasons, the US regretfully suggests that the entry for Germany indicate that it is noncompliant as to preservation for foreign requests.

**Comments by the Federal Ministry of Justice on 25 January 2015**

Under German law the same rules are applicable for national and international cases, § 59 Act On International Cooperation in Criminal Matters. The code of criminal procedure allows the preservation of data. The preservation may be ordered only by the court and, in exigent circumstances, by the public prosecution office. According to our experience, the preservation of data works well in practice (also in international cases).

**Comments by the USA on 3 Februray 2015**

I'm afraid I can't agree that the German preservation arrangement complies with the Convention. If you want preservation, you must make a formal mutual legal assistance request; this is no different than in decades past.

In addition, German practice is wasteful of the time of other countries.
I cannot take on the task of adducing cases for the Ministry. It should talk to the BKA and prosecutors who implement the system. If German law enforcement had to make an MLA request every time it needed US preservation. the problem would be clear pretty quickly.

**Further information provided by the Federal Ministry of Justice on 28 May 2015 in response to the draft assessment report**

Thank you for sharing the draft assessment concerning Germany prepared by the T-CY Bureau. The draft comes to the conclusion, that Germany appears not in line with Articles 29 and 30 of the Budapest Convention. We strongly disagree with this assessment.

Germany's assessment already was completed in 2012 with the result that Germany concerning Article 29 is in line and concerning Article 30 is partially in line with the Budapest Convention (see page 79 of the Assessment Report - document T-CY (2012)10). Given that no legal or factual changes have occurred since then which might negatively affect the implementation of these provision, it seems to be a rather unusual step to reopen Germany´s assessment and to downgrade it in the ensuing follow up process. In addition, as pointed out below, the rewritten assessment is based on a description of Germany´s legal system which is not entirely correct.

Concerning point 2 - Follow up given by Parties to the assessment report 2012:

The description of German law given on page 5 is not entirely accurate. Section 100j of the Criminal Code of Procedure (see appendix) allows for the identification of the holder of a dynamic IP address without requiring a court order. The information may be requested by the public prosecutor or police directly. Only if the request for information refers to data by means of which access to terminal equipment or to storage media is protected, the request must be ordered by the court or, in exigent circumstances, by the public prosecution office or by the police officials assisting it.

In addition, the description of the procedure regarding requests from another party according to Article 29 and 30 is not accurate. The German prosecutors do not ask for a formal request of mutual legal assistance at this early stage. In some cases, they may, however, ask for confirmation of the requesting party's intention to submit a request for mutual legal assistance. This is in line with the Convention. Article 29 para. 1 allows for requests for the preservation of data "in respect of which the requesting party intends to submit a request for mutual assistance". Article 29 para. 2 f specifies that a preservation request shall specify that the requesting party intends to submit a request for mutual legal assistance.

German law provides for a speedy procedure in order to secure the traffic data required. Pursuant to Section 100g (2) and Section 100b (1) of the Criminal Code of Procedure the public prosecution office may issue the necessary order directly when exigent circumstances require it. This is the case when a delay in procedure would bear the risk of loosing important data.

It is true however that in some cases German prosecutors ask for additional case information before making a decision whether they answer the request or not. Germany has availed itself of the reservation provided in Article 29, paragraph 4 of the Budapest convention. Germany may thus refuse the request for preservation in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. To assess dual criminality, German prosecutors need information on the facts of the case. If the information provided by the requesting State is insufficient to assess criminality under German law, German prosecutors will ask for additional information. Compliance with such a request, however, does not require the requesting state to submit a formal request for mutual assistance. A more extensive description of the facts of the case will be sufficient in most cases. Possibly, there are misconceptions on the part of other state parties on this point. Therefore, Germany would appreciate an opportunity to study the cases in which other parties allegedly have made negative experiences. It would be very helpful if specific cases could be given to allow references to enable an analysis of the possible problems.

Concerning point 3 - Update on data retention regulations:

On 27 May 2015, German Federal Government adopted a draft law on mandatory data retention. The draft law provides for the mandatory retention of traffic data for a period of ten weeks and of location data for a period of four weeks. Law enforcement authorities may obtain retained data if

1. facts give rise to the suspicion that a person has committed one of several listed particularly serious criminal offences,

2. the offence is particularly serious in the individual case as well,

3. other means of establishing the facts or determining the accused's whereabouts would be much more difficult or offer no prospect of success and

4. access to the data is proportionate.

By combining a relatively short period of retention with a reduction of the categories of data to be retained and strict access regulation, the planned date retention regime complies with the standards laid down by the European Court of Justice in its judgment of 8 April 2014 (C-293/12 and C-594/12).

Therefore, Germany requests to maintain the previous evaluation in regard to Article 29 with "in line" and in regard to Article 30 with "partially in line".

**Further question sent by the T-CY Secretariat on 3 June 2015 to the Federal Ministry of Justice**

Thank you very much for the additional clarification. Following further discussions with Bureau members, the following comments and questions have come up:

Some general comments:
- Bureau members believe that an assessment can change based on actual experience.
- The preservation provisions of the Budapest Convention cover any type of data, including also content data.
- There are no differences of opinion regarding Articles 16, 17 and 30. The provision in question is Article 29.
- As stated in the draft assessment, this does not mean that Germany is unable to cooperate effectively at international levels with regard to requests not entailing preservation

Some specific questions:

- Subscriber data: The German response is unclear about how effective the legal provisions are in practice. Apparently, in some circumstances, subscriber data may be preserved by a prosecutor or the police. In other circumstances, a court order must be procured. The understanding, for example of the US authorities, is that it must make a formal mutual legal assistance request whenever Germany executes preservation by obtaining a court order. Is this incorrect?

- Traffic data: The response seems to say that traffic data may be preserved by a prosecutor only if exigent circumstances exist, including "when a delay in procedure would bear the risk of losing important data." There is a risk of loss in every case; that's the reason for requesting preservation. Unless exigent circumstances are considered to exist in every case, compliance with Article 29 would not be complete.
Perhaps Germany obtains court orders for the cases in which exigent circumstances are considered to be absent. The understanding, for example of the US, is that it must make a formal mutual legal assistance request whenever Germany executes preservation by obtaining a court order. Is this incorrect?

- Content data: This is not addressed in the response, but is necessary for compliance with Article 29.

- Whether a mutual legal assistance request is required: For example, the US has been advised that it must file a formal mutual legal assistance request every time it requests preservation that Germany fulfills by seizure. The MLA request must be sent when preservation is requested or immediately thereafter. No allowance is made for the fact that circumstances may change - an official may request preservation with the full intention to follow it with an MLA request, but the data may become unnecessary for any number of reasons.
If MLA is required only in fewer circumstances, a Ministry of Justice statement of when they are required might assist in resolving this issue.

- Dual criminality: the German response suggests that Germany is permitted to review every preservation request for dual criminality. This is incorrect under Article 29/4 and paras 285 and 286 of the Explanatory Memo. Could Germany clarify its position?

It would help the Bureau to have your comments on these question.

**Further information provided by the Federal Ministry of Justice on 10 June 2015**

It is incorrect to state that a formal mutual legal assistance request is a requirement, or that obtaining a court order is necessary in every case, before German authorities can preserve data. Search and

seizure upon foreign requests are subject to judicial review but may be ordered without prior court involvement by the public prosecution service or law enforcement agents, pursuant to Section 67 para. 4 of the Act on International Cooperation in Criminal Matters, if a delay poses a threat of data loss (since there is no data retention in Germany, there will be a threat of data loss in most cases). This applies to any type of data.
Furthermore, Section 67 para. 1 explicitly allows preservation measures prior to the receipt of the actual MLA request. Section 67 para. 1 covers any type of data (i.e. Subscriber data, traffic data and Content data).
Should it turn out that preserved data is not needed, it would be a logical consequence that following up with a formal judicial request becomes unnecessary. This does not relieve of the duty to accompany preservation requests with formal MLA in principle. It cannot be inferred from those scenarios that formal MLA would not be a requirement.

I have also asked the Federal Criminal Police Office for an assessment, whether the expedited preservation works in practice. According to their assessment the preservation of data works in practice.

Section 67 of Act on International Cooperation in Criminal Matters - Search and Seizure
(1) Objects that may be considered for handing over to a foreign State may be seized or otherwise secured even prior to the receipt of the request for surrender. To this end, a search may be conducted.
(2) If the conditions specified in s. 66(1) no. 1 and (2) no. 1 apply, objects may also be seized or otherwise secured if necessary for the enforcement of a request which is not directed at the handing over of the objects. Subsection (1) 2nd sentence above shall apply mutatis mutandis.
(3) The Amtsgericht in whose district they are to be performed shall have jurisdiction to order the search and seizure. S. 61(2) 2nd sentence shall apply mutatis mutandis.
(4) If cases of emergency the public prosecution service or its agents (s. 152 of the Gerichtsverfassungsgesetz) may order the search and seizure.
As I said before, it would be good to know, in what cases the preservation of data didn't work out.

**Further question sent by the T-CY Secretariat to the Federal Ministry of Justice on 12 June 2015**

Many thanks. Discussions with BU members are ongoing.

A short, and hopefully final, query: Could you also clarify the matter regarding the dual criminality requirement:

- Dual criminality: the German response suggests that Germany is permitted to review every preservation request for dual criminality. This is incorrect under Article 29/4 and paras 285 and 286 of the Explanatory Memo. Could Germany clarify its position?

**Reply by the Federal Ministry of Justice on 12 June 2015**

Basically there is the requirement of dual criminality under German law.
For offences other than those established in accordance with Art. 2 through 11 of the Convention Germany declared a reservation according to Art. 42.
For offences according to Art. 2 through 11 the requirement of dual criminality does not have any effect in practice since these offences are criminal under German law without exception (thus, the requirement of dual criminality is always met and does not require further consideration).

One more hint: The Federal Police Office had informed me, that (besides § 67 IRG) there are also other possibilities for the expeditous preservation of data: In cases where there are already investigations in Germany the prosecutor can carry out a search or obtain a production order according to the provisions of the code of criminal procedure. In these cases neither a court decision nor a formal MLA request is required and there is also no requirement for dual criminality. In other cases (where there are no investigations in Germany at the time of the request) the prosecutor will open investigations in Germany if the preservation request gives rise to the suspicion of a criminal act and if done so, the police or the prosecutor can also preserve data under the code of criminal procedure (which do not require dual criminality).

## 5.3 Italy

PERSONAL DATA PROTECTION CODE
Legislative Decree no. 196 of 30 June 2003

Section 123
*(Traffic Data)*

1. Traffic data relating to contracting parties and users that are processed by the provider of a public communications network or publicly available electronic communications service shall be erased or made anonymous when they are no longer necessary for the purpose of transmitting the electronic communication, subject to paragraphs 2, 3 and 5.
2. Providers shall be allowed to process traffic data that are strictly necessary for contracting parties' billing and interconnection payments for a period not in excess of six months in order to provide evidence in case the bill is challenged or payment is to be pursued, subject to such additional retention as may be specifically necessary on account of a claim also lodged with judicial authorities.
3. For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred to in paragraph 2 to the extent and for the duration necessary for such services or marketing, on condition that the contracting party or user to whom the data relate has given his/her prior consent. Such consent may be withdrawn at any time.
4. In providing the information referred to in Section 13, the service provider shall inform a contracting party or user on the nature of the traffic data processed as well as on duration of the processing for the purposes referred to in paragraphs 2 and 3.
5. Processing of traffic data shall be restricted to persons in charge of the processing who act – pursuant to Section 30 – directly under the authority of the provider of a publicly available electronic communications service or, where applicable, the provider of a public communications network and deal with billing or traffic management, customer enquiries, fraud detection, marketing of electronic communications or the provision of value-added services. Processing shall be restricted to what is absolutely necessary for the purposes of such activities and must allow identification of the person in charge of the processing who accesses the data, also by means of automated interrogation procedures.
6. The Authority for Communications Safeguards may obtain traffic and billing data that are necessary for settling disputes, particularly with regard to interconnection or billing matters.

Section 132
*(Traffic Data Retention for Other Purposes)*

1. Without prejudice to Section 123(2), telephone traffic data shall be retained by the provider for twenty - four months as from the date of the communication with a view to detecting and suppressing criminal offences, whereas electronic communications traffic data, except for the contents of communications, shall be retained by the provider for twelve months as from the date of the communication with a view to the same purposes.

1-bis. The data related to unsuccessful calls that are processed on a provisional basis by the providers of publicly available electronic communications services or a public communications network shall be retained for thirty days

2.[Repealed.]

3. Within the term referred to in paragraph 1, the data may be acquired from the provider by means of a reasoned order issued by the public prosecutor also at the request of defence counsel, the person under investigation, the injured party, or any other private party. Defence counsel for either the defendant or the person under investigation may directly request the provider to make available the data relating to the subscriptions entered into by his/her client according to the arrangements specified in Section 391-quater of the Criminal Procedure Code without prejudice to the requirements set out in Section 8(2), letter f), with regard to incoming phone calls.

4. [Repealed.]
4-bis. [Repealed.]

4-ter. The Minister for Home Affairs or the heads of the central offices specialising in computer and/or IT matters from the State Police, the Carabinieri, and the Financial Police as well as the other entities mentioned in paragraph 1 of section 226 of the implementing, consolidating, and transitional provisions related to the Criminal Procedure Code as per legislative decree no. 271/1989, where delegated by the Minister for Home Affairs, may order IT and/or Internet service providers and operators to retain and protect Internet traffic data, except for contents data, according to the arrangements specified above and for no longer than ninety days, also in connection with requests lodged by foreign investigating authorities, in order to carry out the pre-trial investigations referred to in the said section 226 of the provisions enacted via legislative decree no. 271/1989, or else with a view to the detection and suppression of specific offences. The term referred to in the order in question may be extended, on grounds to be justified, up to six months whilst specific arrangements may be made for keeping the data as well as for ensuring that the data in question are not available to the IT and/or Internet service providers and operators and/or to third parties.

4-quater. Any IT and/or Internet service providers and/or operators that are the subject of the order mentioned in paragraph 4-ter shall comply without delay and forthwith give assurances to the requesting authority as to their compliance. IT and/or Internet service providers and/or operators are required to keep the order at issue confidential along with any activities performed accordingly throughout the period specified by the said authority. Violation of this requirement shall be punished in accordance with section 326 of the Criminal code unless the facts at issue amount to a more serious offence.

4-quinquies. The measures taken under paragraph 4-ter above shall be notified in writing without delay, in any case by forty-eight hours as from service on the addressee(s), to the public prosecutor that is competent for the place of enforcement, who shall endorse them if the relevant preconditions are fulfilled. The measures shall cease to be enforceable if they are not endorsed.

5. Data processing for the purposes referred to in paragraph1 shall be carried out by complying with the measures and precautions to safeguard data subjects as required under Section 17, which are aimed at ensuring that the retained data fulfil the same quality, security and protection requirements as network data as well as at:
a. providing in all cases for specific systems allowing both computer-based authentication and authorisation of persons in charge of the processing as per Annex B,
b. [Repealed.]
c. [Repealed.]
d. laying down technical mechanisms to regularly destroy the data after expiry of the term referred to in paragraph 1.

Section 132-bis
*(Procedures Established by Providers)*

1. Providers shall establish internal procedures to meet the requests made in compliance with the provisions that envisage access to users' personal data.
2. Upon demand, providers shall provide the Garante, having regard to the respective scope of competence, with information on the procedures referred to in paragraph 1, the number of requests received, the legal justification invoked and their response.

Italian authorities replied:

**Article 16 Expedited preserv.**

We use search and seizure order according to the Italian criminal procedure code.

**Article 17 Preserv. and partial disclosure**

See

Section 132 PERSONAL DATA PROTECTION CODE, Legislative Decree no. 196 of 30 June 2003

3. Within the term referred to in paragraph 1, the data may be acquired from the provider **by means of a reasoned order issued by the public prosecutor** also at the request of defence counsel, the person under investigation, the injured party, or any other private party.

**Article 29 Expedited preserv. (international)**

the requesting party should submit an MLA to Italian authorities.
*In the meanwhile* we can use information provided by a foreign investigation authority via law enforcement channels (ie. Interpol, Europol) or via Eurojust to open a case in Italy, in order to use a search and seizure order iussed by the public prosecutor and preserve electronic evidence.

**Article 30 Preserv. and partial disclosure (international)**

See

Section 132 PERSONAL DATA PROTECTION CODE, Legislative Decree no. 196 of 30 June 2003

4-ter. The Minister for Home Affairs or the heads of the central offices specialising in computer and/or IT matters from the State Police, the Carabinieri, and the Financial Police as well as the other entities mentioned in paragraph 1 of section 226 of the implementing, consolidating, and transitional provisions related to the Criminal Procedure Code as per legislative decree no. 271/1989, where delegated by the Minister for Home Affairs, may order IT and/or Internet service providers and operators to retain and protect Internet traffic data, except for contents data, according to the arrangements specified above and for no longer than ninety days, **also in connection with requests lodged by foreign investigating authorities**, in order to carry out the pre-trial investigations referred to in the said section 226 of the provisions enacted via legislative decree no. 271/1989, or else with a view to the detection and suppression of specific offences. The term referred to in the order in question may be extended, on grounds to be justified, up to six months whilst specific arrangements may be made for keeping the data as well as for ensuring that the data in question are not available to the IT and/or Internet service providers and operators and/or to third parties.

4-quater. Any IT and/or Internet service providers and/or operators that are the subject of the order mentioned in paragraph 4-ter shall comply without delay and forthwith give assurances to the requesting authority as to their compliance. IT and/or Internet service providers and/or operators are required to keep the order at issue confidential along with any activities performed accordingly throughout the period specified by the said authority. Violation of this requirement shall be punished in accordance with section 326 of the Criminal code unless the facts at issue amount to a more serious offence.

4-quinquies. The measures taken under paragraph 4-ter above shall be notified in writing without delay, in any case by forty-eight hours as from service on the addressee(s), to the public prosecutor that is competent for the place of enforcement, who shall endorse them if the relevant preconditions are fulfilled. The measures shall cease to be enforceable if they are not endorsed.

### 5.4 Lithuania

**Article 16 – Expedited preservation of stored computer data**

Art 65 Para 2 of the LEC sets out an obligation to public communication network and (or) service providers to preserve and disclose, in accordance with the procedures established by the law and for the purposes of prevention, disclosure and investigation of criminal offences, to competent authorities the data generated and processed by them. The data to be preserved and disclosed are specifically listed in Annex to the LEC:

1. Data necessary to trace and identify the communication source;
2. Data necessary to identify the communication destination;
3. Data necessary to identify the date, time and duration of a communication;
4. Data necessary to identify the type of communication;
5. Data necessary to identify user's communication equipment or what purports to be their equipment;
6. Data required to identify the location of mobile communications equipment.

Based on Art 66 Para 6 and Art 77 Para 3, data preservation period is 6 months with a possibility to extend the period for no longer than another 6 months on a request of competent authorities (criminal intelligence, pre-trial investigation entities).

Providers of public communication networks and services shall store data referred to above in accordance with the following principles:

1) The data must be of the same quality and subject to the same security and protection requirements as those data on the network;
2) Data are subject to appropriate technical and organisational measures to protect them against accidental or unlawful destruction, accidental loss or alteration, or unauthorised or unlawful storage, processing, access or disclosure;
3) Data are subject to appropriate technical and organisational measures to ensure that authorised personnel can obtain access to them only.

At the end of the retention period, the stored data must be destroyed. Supervision over the legality of the processing of personal data shall be exercised in the field of electronic communications pursuant to the laws and other legal acts regulating the processing of data and the protection of privacy.

In accordance with the Lithuanian legislation, competent authorities have several legal grounds and means to obtain the data stored by communication network and service providers, and thus secure electronic data for further use for prevention, disclosure and investigation of criminal offences.

Main legal acts, providing for these means are:

1) The Criminal Procedure Code of the Republic of Lithuania (CPC).
2) The Law on Criminal Intelligence (LCI) (that replaced the Law on Operational Activities, indicated in 2012 Assessment Questionnaire);
3) The Law on Cyber Security of the Republic of Lithuania (LCS) (adopted on 11 December 2014) along with Rules of Procedure on Provision of Information, Necessary for Prevention and Investigation of Cyber Incidents Likely to Have Characteristics of a Criminal Offence, to the Police, on Implementation of Police Requirements, and on Investigation of Cyber Incidents, approved by the Order of the Lithuanian Police Commissioner General (Rules of Procedure on Cyber-Incidents).

Respectively, stored data may be obtained within the scope of three types of investigations: (1) pre-trial investigation; (2) criminal intelligence investigation; or (3) cyber incident investigation.

In a pre-trial investigation, based on respective provisions of the CPC, the following means may be used:

- Art 145 – Search;
- Art 147 – Seizure;
- Art 154 – Control, Recording and Accumulation of Information Transmitted through Electronic Communications Networks (for live interception of content data);
- Art 155 – Public Prosecutor's Right to get acquainted with the Information (to obtain stored data).

In a criminal intelligence investigation, based on respective provisions of the LCI, the following means may be used:

- Art 9 of the LCI, criminal intelligence entities may obtain for criminal intelligence purposes without a court ruling information directly related to telephone communication numbers or terminal equipment of the electronic communication network, to the affiliation of a telephone communication number, e-mail address or terminal equipment of a network, the account numbers of a natural or legal person or the affiliation of bank accounts and (or) financial instruments and (or) means of payment and the persons authorised to have it at their disposal. To obtain traffic and content data a court ruling or approval is required.
- Articles 2 and 10, criminal intelligence entities are vested with the right to use technical means for the purposes of criminal intelligence. Technical means may be used in accordance with the general procedure, when they are used for recording information during surveillance in public places, in premises and vehicles at the initiative of entities of criminal intelligence in order to ensure internal security; also technical means may be used in accordance with the special procedure, when they are used on the basis of a reasoned court ruling to monitor or record economic, financial operations of a natural or legal person, the use of financial instruments and (or) means of payment, personal conversations, other communication or actions, where none of the participants in the conversation, other communication or actions are aware of such monitoring. This method may be used for legal interception of electronic data.

Criminal intelligence as such aims at prevention and detection of criminal acts, identification of the persons planning, committing or having committed these acts, protection of persons against criminal influence, search for the individuals who are hiding from pre-trial investigation or trial, convicted or

missing persons, also at search for items, money, securities and other property related to commission of criminal acts, and ensuring the internal security of criminal intelligence entities.

Criminal intelligence investigation may be initiated and conducted if:

1) Criminal intelligence entities become aware of the information about a grave or serious crime or less serious crime specifically listed in the LCI is being planned, being committed or having been committed, or about persons who are planning, committing or having committed these criminal acts.
2) A suspect, an accused or a convicted person hides.
3) A person is reported missing.
4) Protection of persons against criminal influence is being implemented.

In an investigation of a cyber-incident, Cybercrime Board of the Lithuanian Criminal Police Bureau (also a 24/7 Point of Contact under the Budapest Convention on Cybercrime), based Art 12 of the LCS and Para 10 of the Rules of Procedure on Cyber-Incidents, has the right to send lawful requests to the providers of communication networks and services to provide data that is necessary to prevent and (or) investigate a cyber-incident that has the characteristics of a criminal offence. For these purposes, Cybercrime Board shall send a filled out form to the provider.

**Article 17 – Expedited preservation and partial disclosure**

Based on Art 77 Para 1 of the LEC, economic entities providing electronic communication networks and (or) services, shall, in accordance with the procedures established by the law, disclose immediately the information that is available to them and which is necessary to prevent, investigate and detect criminal offences, to the requesting competent authorities (criminal intelligence, pre-trial investigation entities, public prosecutors, judges) on the basis of their request.

On top of the means mentioned above, provision of data and other information, necessary for prevention and investigation of criminal offences, in Lithuania is also broadly based on voluntary cooperation between the law enforcement and private sector, in particular, the larger public communication service providers and financial institutions. Therefore, data preservation and partial disclosure is efficiently implemented.

**Art 29 – Expedited Preservation of Stored Computer Data (international), Art 30 – Expedited Disclosure of Preserved Traffic Data**

For the purposes of an effective implementation of international commitments established in the Budapest Convention on Cybercrime, in 2011, Cybercrime Board of the Lithuanian Criminal Police Bureau was appointed as 24/7 Point of Contact for urgent cooperation in the field of fight against cybercrime. It also serves as a point of contact for the purposes of cooperation within the scope of Directive 2013/40/EU and G7 Network.

In accordance with its competence, Cybercrime Board is authorised to send/receive and follow up to data preservation requests. Upon receipt of a request from a foreign point of contact, it has the right to send out lawful requests to Lithuanian entities to preserve data available to them and obtain data and other information disclosure of which does not require court rulings (basic subscriber information, partially traffic data). Should data or other information the disclosure of which requires court ruling be needed, an MLAT procedure should be applied.

Both, the Code on Criminal Procedure and the Law on Criminal Intelligence allows the Lithuanian law enforcement to cooperate with the law-enforcement institutions of foreign states and with

international organisations, EU agencies, to provide support to each other, and to exchange intelligence and other information. This provides for the grounds to disclose stored data.

Expedited data preservation tool as provided in Art 29 of the Budapest Convention is effectively used in Lithuania as both the requested and the requesting party. In average, 20-30 preservation requests from other states are processed and 10-15 sent to foreign countries annually by Cybercrime Board. Main countries for cooperation: Belarus, Germany, Latvia, Moldova, the Netherlands, Romania, Ukraine, United Kingdom, USA.

## 5.5 Slovakia

**Section 69 d**

**Provision and disclosure of personal data**

(1) The Police Corps shall provide and disclose personal data to other authorities or persons if
a) provided by a law,
b) it is for the benefit of a person whose personal data are stored, and if that person gave a consent to provision or disclosure,
c) the provision or disclosure of personal data is necessary to eliminate an imminent serious threat to safety of persons or to public order or
d) it is regulated by a specific regulation 27dd) or an international treaty binding the Slovak Republic.

(2) The Police Corps shall upon written request provide the Member State of the European Union with personal data of persons that may be important to assess whether the person represent a risk to the public order or security. The Police Corps shall provide personal data within two months of receipt of the written request.

(3) The Police Corps shall provide or disclose pursuant to paragraph 1 a), b) and d) personal data upon written request or contract, which must include the purpose for which personal data are to be provided or made available; if the provision asks the Slovak Intelligence Service, the application does not contain a purpose for which personal data are to be provided or made available. The Police Corps may provide or make available personal data under paragraph 1 c) to other authorities or persons without prior written request; authority or person to whom the data provided or made available shall within three days after the impediment that prevented the delivery of a written application submit a written request to the Police Corps.

(4) The provision and disclosure of personal data must be accompanied by information on final decisions of law enforcement agencies, if this information is related to such data.
(5) The recipient of data referred to in paragraphs 1 to 4 shall be entitled to process personal data for a purpose other than for which it was provided or made available only with the prior consent of the Police Corps; it does not apply, when there is no purpose stated in the application. If the data recipient under paragraphs 1 to 4 is asked for information how these data are processed, by the Police Corps, he is obliged to inform the Police Corps in written within 14 days.

(6) Personal data may be also provided and disclosed abroad without a written request if so provided by law, special regulation 27dd) or an international treaty binding the Slovak Republic.

(7) The Police Corps can the provision and disclosure of personal data to other authorities or persons specify the time after which the beneficiary is obliged to delete, block dispose or verify whether personal data are still necessary for him.

(8) The Police Corps may personal data received from the Member State authority provide or disclose to persons who are not public authorities only with the prior consent of the Member State authority that personal data provided or made available, if the provision or disclosure of personal data is not in conflict with the interests of the person concerned and if such provision or disclosure is essential to
a) fulfillment of task according to the law,
b) prevention and detection of crime and detection of perpetrators of criminal offences, criminal investigation, prosecution of criminal offences and enforcement of judgments in criminal proceedings,
c) the prevention of imminent serious threat to public order or national security or
d) the prevention of serious human rights violations of natural persons.

(9) The Police Corps shall instruct another authority or a person with whom provided or disclosed personal data that they may be processed only for the purpose for which it was provided or disclosed.

(10) Member States of the European Union pursuant to paragraph 2 shall also mean another State Party to the Agreement on the European Economic Area and Swiss Confederation.

### 5.6 Slovenia

Regarding expedited preservation provisions two important developments should be noted:

1. Ministry of Justice proposed some changes in Criminal Procedure Code in
article 149/b:
- they proposed that word "provider" would be added after the word"operator". The reason is that the law enforcement at the moment don'thave any clear provisions in CPC that they can demand data (i.e. trafficdata, subscriber data etc.) from companies or individuals who offers some sort of internet or other communications services.
At the moment we have in article 149/b the term "operator of the electronic communications network" which concerns only registrated operators (internet service providers and stationary/mobile phone service providers). According to this proposed change we think that law enforcement will obtain (and also preserve) data much faster and easier from any subject who offers services on internet and therefore has some kind of data. Of course this proposed changes of CPC provisions are not in direct connection with expedited preservations but we hope that this procedures will also be more easier and clear. The proposal is still in parlament procedure.
In the meantime we had two requests from other parties/EU members for expedited preservation and we did it successfully.

2. Our Constitutional Court repealed the section in our Electronic Communication Act regarding data retention. They lean their decision on EU Court which also repealed EU Data Retention Directive. So all the internet and mobile providers/operators were required to erase all data. Now they can only store data for their billing needs - this sort of data are usualy stored for period of max three month (but this period also differs among operators/providers). Before they were obliged to store data for 12 months (data for stationary & mobile phone services) and for 8 months (data for internet services). There are many things unclear right now, so we hope that we will have more information on obtaining data in the future.

## 5.7 Spain

**REPORT ON ONGOING LEGAL REFORMS WITH REGARD TO THE IMPLEMENTATION OF ARTICLES 16, 17, 29 AND 30 OF BUDAPEST CONVENTION.**

As regards Article 16 of Budapest Convention, a Draft Bill amending the Criminal Procedural Law is currently being under parliamentary scrutiny and most likely will be passed in the second semester of 2015. One of the objectives of this Draft Bill is the regulation of technological investigation measures.

In the Draft Bill a provision, whereby the data retention order is regulated, has been introduced. According to this provision, the Prosecutor or the Law Enforcement Units are entitled to request from any person or legal entity the retention and protection of data or concrete information available to them until judicial authorization is granted. The requested persons / entities are obliged to cooperate, comply with the order and are bound by an obligation of confidentiality; otherwise they might incur in criminal liability for a disobedience crime.

As for Article 17 of the Budapest Convention, as already stated in previous questionnaires, the Spanish data retention Law, *Law 25/2007 on the Retention of Data Generated or Processed in Connection with Electronic or Public Communications Networks*, establishes an obligation for telecommunications providers to retain and store data for a period of one year.

Under the current legal framework, the possibility to access retained data is limited to serious crimes; the concept of seriousness has been construed by the Courts in some law cases in a not very consistent way and sometimes with a contradictory jurisprudence. Having said so, the abovementioned ongoing procedural reform, fully solves the issue due to the fact that it envisaged the access to retained data related to investigations on crimes committed via electronic means or any IT tools, always with the judicial authorization.

The Draft Bill states, that access to electronic data retained, always linked to a communication process, by providers of communication services / operators or subjects can only be granted with the previous judicial authorization

As regards Articles 29 and 30 of the Budapest Convention, the forthcoming legal framework will allow for the preservation of electronic data and the retention of traffic data and the access to retained information, under domestic legal requirements, when requested by a competent foreign authority in the context of Treaties and Conventions ratified by Spain.

**REPORT ON THE NATIONAL FRAMEWORK ON ELECTRONIC COMMUNICATIONS DATA RETENTION.**

The Data Retention Directive, 2006/24/CE, was transposed into national legislation by Law 25/2007 of October 18. This Domestic Data Retention Law is currently valid and enforceable; and its compliance with constitutional standards has not been challenged until now.

As regard to this matter, it should be noted that the Law 25/2007 provides for very strict measures concerning to the protection and access to retained information. Such measures can be summarized as follows:

a) The regime for the protection and security of stored data is governed by the Data Protection Law and is realized under the supervision of the Data Protection Spanish Agency. Thus, Article 10 of Law 25/2007 lists a number of infringements, graduated according to their seriousness, whenever the obligations are breached.

b) Judicial authorization is needed to have access to retained data; pursuant Article 7.2 such authorization will have to be adopted following the procedure established in the Procedural Criminal Law, such judicial decision, under necessity and proportionality criteria, should specify the particular retained data who can be delivered to the authorized agents

- Pursuant Article 6.2 of the Law, only the needed information should be released.

c) Such judicial decision can only be delivered in criminal proceedings for the investigation of serious forms of criminality. The abovementioned Draft Bill will include a list of crimes in which investigation such intrusive measure can be adopted.

d) The data can only be provided to authorized officials and within the deadline established by the law.

e) The data should be retained for a period of 12 years (somewhere in between the range of 6 and 26 months foreseen in the Directive); nevertheless Article 5.1 provides for the possibility of reducing or extending such period by means of by-laws after consultation with providers / operators for certain category of data (max 24 months, min 6 months) taking into consideration storage and conservation costs as well as the interest of such data for the investigation, detection and bringing to trial serious crimes.

That is why, although data retention is always mandatory in all cases and with respect to all citizens with no distinction, i.e. there is no prior selection of data to be retained (this would be a difficult task to conduct), existing controls and safeguards guarantees the security / secrecy of the information in order to grant access only in the specific cases where is necessary according to proportionality criteria.
This framework provides for sufficient safeguards and minimizes the risk of privacy and personal data protection being unjustly affected, that is why the Law to this day remains valid without prejudice of future initiatives the Government or the Legislative Power might take.

## 5.8 "The Former Yugoslav Republic of Macedonia"

The New CPC (Official gazette 150/2010) have new articles regarding the Article 17 Preservation and partial disclosure and Article 30 Preservation and partial disclosure from the Convention.
Articles 184, 198, 252 paragraphs 1, 4, 5 and 6. Also the Law for international cooperation in criminal matters (Official gazette 124/2010) have articles regarding the international cooperation between the state official body's, articles 15, 25 and 29.

CPC
Art. 184:
Searching the computer system and computer data
(1) At the request of the person who executes the warrant, person who uses computer or have access to it or to another device or data carrier is obliged to access to them and provide the necessary information for a uninterrupted achieving the purpose of the search.
(2) At the request of the person executing of the warrant, the person using the computer or have access to it or to another device or data carrier is obliged immediately take measures to prevent the destruction or alteration of data.
(3) A person who uses a computer or have access to it or to another device or data carrier who resist to act by paragraphs (1) and (2) of this member, the Pre- trail Judge to penalties under the provisions of Article 88 paragraph (1) of this Act.

Article 198
Temporary seizure of computer data
(1) The provisions of Articles 194 paragraph (1), Article 195 paragraph (1) and 197 of this Law apply to the data stored in the computer and related devices for automatic, or data processing devices that are used for collecting and data transfer, data carriers and subscriber information that are available for the provider of the specified service. Upon written request by the public prosecutor, those taken data must be given to the Public Prosecutor within the time he determined. In case of refusal, it shall be dealt with under Article 196 paragraph (1) of this Act.
(2) The Pre-Trial Judge on the proposal of the public prosecutor can determine the size and storage of the computer data under Article 185 of this law if it is necessary, a maximum of six months. After this period, the data will be returned, unless involved in such a crime damage and unauthorized entry into a computer system Article 251 of the Computer Fraud, Article 251-B and Computer and forgery Article 379-a of the Criminal Code, if not included in the performance of another crime with the help of a computer and if they do not serve as proof of crime.
(3) Against the design of the Pre-Trail Judge in which a certain

measures under paragraph (2) of this Article are deafened, the person using the computer and the service provider is entitled to appeal within 24 hours. For the Appel, the competition court is Council under Article 25 paragraph (5) of this Law. The appeal does not suspend execution.

Article 252 (part of the article connected to the cybercrime issues)
Special investigative measures
Purpose and types of special investigative measures
(1) When it is likely to provide information and evidence necessary to successful criminal procedure, which otherwise cannot be collect, it can be taken the following special investigative measures:
1) monitoring and recording of telephone and other electronic communications in the special procedure established by law;
4) Search and secret insight into a computer system;
5) automatic or otherwise, search and compare personal data;
6) inspect the generated telephone and other electronic communications,

International legal assistance

Definition

Article 15 (part of the article connected to the cybercrime issues)
International legal assistance includes:
- Spontaneous delivery information
- The exchange of certain information and notices

Article 25
Spontaneous delivery information
(1) Domestic judicial authority may, under the condition of reciprocity, without official MLA request of the foreign competent authority, to submit information refer to crimes that are collected during its own investigations if considered that the submission of such information could help initiating or conducting an investigation or trial or if you would could lead to the filing MLA request for international legal assistance.
(2) Domestic judicial authority will ask the foreign competent authority to whom this information is submitted under paragraph (1) of this Article a report for each report action taken on the basis of information and delivery of a copy of decisions.
(3) Domestic judicial authority which supplied the information under paragraph (1) of this article, in accordance with regulations to protect personal data can set appropriate conditions for their use in the foreign country in which submitted.

Article 29
Temporary measures

(1) Domestic judicial authority at the request of a foreign competent authority take temporary measures to collect evidence and ensuring evidence already collected or for the protection of threatened legal interests.
(2) Acting under the MLA request of paragraph (1) of this Article a domestic judicial authority may act or partial execution, or the executing of the MLA request can be time limited.