

www.coe.int/TCY

Strasbourg, version 19 May 2016

T-CY (2015)24

Cybercrime Convention Committee (T-CY)

Draft Assessment report

Implementation of the preservation provisions of the Budapest Convention on Cybercrime

Supplementary report for Malta and Panama

Document prepared by the Bureau for consideration by T-CY 15 (24-25 May 2016)

Contents

1	Introduction	3
2	Note on criteria used for the assessment	4
3	Implementation of Articles 16 and 29 on expedited preservation	6
4	Implementation of Articles 17 and 30 – Expedited preservation and partial disclosure of traffic data (domestic/international)	10
5	Data preservation versus data retention	17
6	Conclusions	17
7	Appendix: Replies to questionnaire	19

Contact

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

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

1 Introduction

The 8th Plenary of the Cybercrime Convention Committee (T-CY) in December 2012 adopted a report assessing the implementation of the expedited preservation provisions of the Budapest Convention on Cybercrime by the Parties:¹

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

31 Parties participated in the exercise in 2012.

The 11th (June 2014) and 12th (December 2014) Plenaries reiterated the importance of full implementation of the expedited preservation provisions. The T-CY, therefore, decided to repeat the exercise for Parties that did not participate in assessment in 2012, namely for:

1. Australia
2. Austria
3. Belgium
4. Czech Republic
5. Denmark
6. Dominican Republic
7. Iceland
8. Japan
9. Malta
10. Mauritius
11. Panama

Replies were received from all of these countries, with the exception of Malta and Panama.

The 13th Plenary of the Cybercrime Convention Committee (T-CY) in June 2015 adopted a supplementary report assessing the implementation of the expedited preservation provisions of the Budapest Convention on Cybercrime by the eleven above mentioned countries, with the remark that for Malta and Panama, no replies have been received.²

T-CY regretted that no replies have been received from Malta and Panama and called on all Parties to actively participate in future assessments in the interest of the effectiveness of the Budapest Convention and of efficient international cooperation against cybercrime.

Following 13th Plenary of the Cybercrime Convention Committee (T-CY), Malta's and Panama's authorities replied the questionnaire.

The present draft report provides an assessment of Malta and Panama implementation of the expedited preservation provisions of the Budapest Convention on Cybercrime.

The present draft report was prepared for consideration T-CY 15 (24-25 May 2016).

¹ [http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY\(2012\)10_Assess_report_v31_public.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)10_Assess_report_v31_public.pdf)

² <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b>

2 Note on criteria used for the assessment

In the 2012 assessment, the following criteria were used to assess implementation of Article 16 by the Parties:³

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

As indicated in the report as adopted in December 2012:

Discussions during the T-CY Plenary in December 2012 showed that Parties have different views as to whether a Party meets the requirements of the Budapest Convention if, in the absence of specific preservation orders, powers such as search, seizure or production orders are used. Most Parties would agree that such an approach is valid if such powers indeed permit to secure electronic evidence in relation to any crime and any legal or physical person holding data in an expedited manner.

Some Parties, on the other hand, are of the opinion that (a) the Budapest Convention allows for search, seizure and similar as alternatives to preservation, and that (b) such powers may be limited in line with Article 15 (conditions and safeguards). The assessments in the present report are based on the first approach:

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

In its “conclusions and recommendations”⁴ the T-CY adopted the following position:

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

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

5. Furthermore, greater legal certainty for preservation requests may help improve cooperation between law enforcement and service providers. Recommendation: Even if current systems allow for securing electronic evidence in an expedited manner, Parties should consider the adoption of

³ See page 7 of [http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY\(2012\)10_Assess_report_v31_public.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)10_Assess_report_v31_public.pdf)

⁴ Page 77ff.

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.

Experience since the adoption of the initial report supports these conclusions and recommendations. Several Parties indicated problems when requesting data preservation under Article 29 in Parties that do not dispose of domestic specific preservation provisions in line with Article 16. In such cases, Parties are often required to resort to mutual legal assistance requests or provide a sufficient amount of information to permit search, seizure or production orders in the requested State or to meet the dual criminality requirement. Data may be lost by the time these conditions are met. The requested State would thus not be in line with Article 29. The purpose of expedited preservation is to secure data and allow for the time needed to verify such requirements.

3 Implementation of Articles 16 and 29 on expedited preservation

Party	Legal provisions and practical experience	T-CY Assessment
Malta	<p>Chapter 9 of the Laws of Malta, Criminal Code</p> <p>346. (1) It is the duty of the Police to preserve public order and peace, to prevent and to detect and investigate offences, to collect evidence, whether against or in favour of the person suspected of having committed that offence, and to bring the offenders, whether principals or accomplices, before the judicial authorities.</p> <p>(2) Notwithstanding the generality of subarticle (1), where authorised by law and in the manner so provided, the Police may delay its immediate intervention for the prevention of the commission of an offence.</p> <p>355AD. (1) Where, in the course of an investigation, a person attends voluntarily at, or accompanies a police officer to, a police station or office, that person shall be free to leave at any time, unless and until he is informed that he is under arrest.</p> <p>(2) Where an inspector of Police has a reasonable suspicion that the person who attended voluntarily at the police station or office may have committed an offence subject to imprisonment, he may arrest such person forthwith without warrant and inform him accordingly. The time of the arrest shall be immediately recorded and immediate notice thereof shall be given to a Magistrate.</p> <p>(3) The Police may, orally or by a notice in writing, require any person to attend at the police station or other place indicated by them to give such information and to produce such documents as the Police may require and if that person so attends at the police station or place indicated to him he shall be deemed to have attended that police station or other place voluntarily. The written notice referred to in this subarticle shall contain a warning of the consequences of failure to comply, as are mentioned in subarticle (5).</p> <p>(4) Any person who is considered by the police to be in possession of any information or document relevant to any investigation has a legal obligation to comply with a request from the police to attend at a police station to give as required any such information or document: Provided that no person is bound to supply any information or document which tends to incriminate him.</p> <p>(5) A person who fails to comply with a notice in writing as is referred to in subarticle (3) or</p>	<p>Article 16</p> <p>Malta is in line with this Article. Preservation powers are available for traffic data held by providers. Other powers are available for content data and natural persons.</p> <p>Article 29</p> <p>Malta is in line with this Article.</p>

Party	Legal provisions and practical experience	T-CY Assessment
	<p>who fails, upon being so requested, even if only orally, to accompany voluntarily a police officer to a police station or other place indicated by the police officer for any purpose mentioned in the said subarticle (3) shall be guilty of a contravention punishable with detention and shall be liable to be arrested immediately under warrant.</p> <p>(6) The notice mentioned in subarticle (3) may be served with urgency in cases where the interests of justice so require.</p> <p>(7) A person who attends voluntarily as mentioned in subarticle (3) may be kept apart from any other person, but shall not be kept in any place normally used for the detention of arrested persons.</p> <p>355E. (1) Saving the cases where the law provides otherwise, no police officer shall, without a warrant from a Magistrate, enter any premises, house, building or enclosure for the purpose of effecting any search therein or arresting any person who has committed or is reasonably suspected of having committed or of being about to commit any offence <u>unless</u> -</p> <p>the offence is a crime other than a crime punishable under the Press Act and <u>there is imminent danger that</u> the said person may escape or that <u>the corpus delicti or the means of proving the offence will be suppressed; or</u></p> <p>.....</p> <p>355H. No warrant of entry and search may be executed after sunset unless the Magistrate has otherwise authorised in the warrant, or <u>unless the executing Police officer has reasonable cause to believe that the purpose of the entry and search will be frustrated if the execution of the warrant is delayed.</u></p> <p>355Q. The Police may, in addition to the power of seizing a computer machine, require any information which is contained in a computer to be delivered in a form in which it can be taken away and in which it is visible and legible.</p> <p>357. Where an officer of the Executive Police discovers any weapon, document, trace or vestige or any other thing relating to an offence, he shall take steps to establish and ensure</p>	

Party	Legal provisions and practical experience	T-CY Assessment
	<p>the existence and the preservation thereof in the state in which it was found until he shall have reported the matter to the Court of Magistrates, and, if unable to establish and ensure such existence or preservation, he shall observe the same procedure provided for the drawing up of a "repertus".</p> <p>558. (1) On the discovery of any document relating to any offence , steps shall be taken to secure the existence and preservation thereof, and a procès-verbal, to be known as "repertus", shall be drawn up.</p> <p>(2) The expression "document" includes any paper and any material object which may furnish information, explanation, or other evidence about the offence, or about the guilt or innocence of the accused.</p> <p>Subsidiary Legislation 440.01, PROCESSING OF PERSONAL DATA (ELECTRONIC COMMUNICATIONS SECTOR)</p> <p>19. (1) Data retained under this Part shall be disclosed only to the Police or to the Security Service, as the case may be, where such data is required for the purpose of the investigation, detection or prosecution of serious crime.</p> <p>(2) When data retained under this Part is required, such data shall be provided by a service provider of publicly available electronic communications services or of a public communications network, from whom it is required, in an intelligible form and in such a way that it is visible and legible.</p> <p>(3) A request for data shall be made in writing and shall be clear and specific: Provided that where the data is urgently required, such request may be made orally, so however that the written request shall be made at the earliest opportunity.</p> <p>(4) Data retained under this Part shall, following the request, be provided without undue delay.</p> <p>22. (1) The Police may, in addition to the request for data under regulation 19, issue a conservation order in relation to the data.</p> <p>(2) The conservation order shall be served on the service provider within the retention period applicable under regulation 21.</p> <p>(3) Where a conservation order has been issued, the service provider shall conserve the data -</p> <p>(a) either for a period of six months in addition to the original or extended applicable retention period which period shall not, without an order of a Magistrate or of a competent Court, exceed</p>	

Party	Legal provisions and practical experience	T-CY Assessment
	<p>a total period of two years; or</p> <p>(b) where criminal proceedings have been commenced within the applicable retention period or within such period as extended in accordance with paragraph (a), for such time as may be necessary for the conclusion of the criminal proceedings where the data is required to be produced as evidence; such conclusion shall be deemed to occur when the judgment in the proceedings becomes final and conclusive, whichever is the longer period.</p>	
Panama	<p>In Panama, the following acts are in force:</p> <p>Penal Code of the Republic of Panama (Articles 289, 290, 291 and 292 – there is a new draft law that will amend the Code and will add some more provisions);</p> <p>Law 23/1986 - infringements related with drugs (Article 46: Centro Nacional de Informática Policial);</p> <p>Law 42/2000 (measures regarding prevention of money laundering);</p> <p>Law 6/2002 (regarding transparency on the public management and on confidential information);</p> <p>Law 16/2004 (prevention of the sexual exploitation – including minors and teenagers);</p> <p>Law 15/2008 (informatics in the judicial procedures);</p> <p>Law 51/2008 (conservation, protection and providing of subscribers information of the data of the telecommunications costumers);</p> <p>Law 82/2012 (Electronic signature);</p> <p>Law 83/2012 (use of electronic media in the governmental procedures);</p> <p>Law 121/2013 (amending the Penal Code regarding interception of communications and seizure of data).</p> <p>Even if it is recognised the importance of obtaining electronic evidence, general and “classic” rules still apply, as there is not in place, yet, a specific framework regarding obtaining digital evidence.</p>	<p>Article 16</p> <p>Panama is partially in line with this Article.</p> <p>Article 29</p> <p>Panama is not in line with this Article.</p> <p>The T-CY requests the authorities of Panama to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.</p>

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

Party	Legal provision and practical experience	Assessment
Malta	<p>Chapter 9 of the Laws of Malta, Criminal Code</p> <p>649. (1) Where the Attorney General communicates to a magistrate a request made by a judicial, prosecuting or administrative authority of any place outside Malta or by an international court for the examination of any witness present in Malta, or for any investigation, search or/and seizure, the magistrate shall examine on oath the said witness on the interrogatories forwarded by the said authority or court or otherwise, and shall take down the testimony in writing, or shall conduct the requested investigation, or order the search or/and seizure as requested, as the case may be. The order for search or/ and seizure shall be executed by the Police. The magistrate shall comply with the formalities and procedures indicated in the request of the foreign authority unless these are contrary to the public policy or the internal public law of Malta.</p> <p>(2) The provisions of subarticle (1) shall only apply where the request by the foreign judicial, prosecuting or administrative authority or by the international court is made pursuant to, and in accordance with , any treaty, convention, agreement or understanding between Malta and the country, or between Malta and the court, from which the request emanates or which applies to both such countries or to which both such countries are a party or which applies to Malta and the said court or to which both Malta and the said court are a party. A declaration made by or under the authority of the Attorney General confirming that the request is made pursuant to, and in accordance with, such treaty, convention, agreement or understanding which makes provision for mutual assistance in criminal matters shall be conclusive evidence of the matters contained in that certificate. In the absence of such treaty, convention, agreement or understanding the provisions of subarticle (3) shall be applicable.</p> <p>(3) Where the Minister responsible for justice communicates to a magistrate a request made by the judicial authority of any place outside Malta for the examination of any witness present in Malta, touching an offence cognizable by the courts of that place, the magistrate shall examine on oath the said witness on the interrogatories forwarded</p>	<p>Article 17</p> <p>Malta is not in line with this Article.</p> <p>Article 30</p> <p>Malta is not in line with this Article.</p> <p>The T-CY requests the authorities of Malta to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.</p>

Party	Legal provision and practical experience	Assessment
	<p>by the said authority or otherwise, notwithstanding that the accused be not present, and shall take down such testimony in writing.</p> <p>(4) The magistrate shall transmit the deposition so taken, or the result of the investigation conducted, or the documents or things found or seized in execution of any order for search or/and seizure, to the Attorney General.</p> <p>(5) For the purposes of subarticles (1) and (3) the magistrate shall, as nearly as may be, conduct the proceedings as if they were an inquiry relating to the in genere but shall comply with the formalities and procedures indicated by the requesting foreign authority unless they are contrary to the fundamental principles of Maltese law and shall have the same powers, or as nearly as may be, as are by law vested in the Court of Magistrates as court of criminal inquiry, as well as the powers, or as nearly as may be, as are by law conferred upon him in connection with an inquiry relating to the "in genere": provided that a magistrate may not arrest any person, for the purpose of giving effect to an order made or given under article 554(2), or upon reasonable suspicion that such person has committed an offence, unless the facts amounting to the offence which such person is accused or suspected to have committed amount also to an offence which may be prosecuted in Malta.</p> <p>(5A) If the request cannot, or cannot fully, be executed in accordance with the formalities, procedures or deadlines indicated by the requesting foreign authority, the requesting authority shall be informed indicating the estimated time within which or the conditions under which execution of the request may be possible.</p> <p>(5B) The proceedings referred to in this article shall, as nearly as may be, be conducted as if they were an inquiry relating to the "in genere".</p> <p>(6) Where the request of the foreign authority is for the hearing of a witness or expert by video-conference, the provisions of subarticles (7) to (12), both inclusive, shall apply.</p> <p>(7) The magistrate shall summon the person to be heard to appear at the time and place equipped with videoconference facilities appointed for the purpose by the magistrate. The magistrate shall give effect to any measures for the protection of the person to be heard which the Attorney General may declare to have been agreed upon with the requesting foreign authority.</p>	

Party	Legal provision and practical experience	Assessment
	<p>(8) The magistrate shall conduct the hearing and where necessary the magistrate shall appoint an interpreter to assist during the hearing. The magistrate present shall ensure that the person to be heard is identified and that the proceedings take place and continue at all times in conformity with the fundamental principles of the law of Malta.</p> <p>(9) The person to be heard may claim the right not to testify which would accrue to him or her under the law of Malta or under the law of the country of the requesting foreign authority.</p> <p>(10) Subject to any measures for the protection of the person to be heard referred to in subarticle (7), the magistrate shall on the conclusion of the hearing draw up minutes indicating the date and place of the hearing, the identity of the person heard, the identities and functions of all other persons participating in the hearing, any oaths taken and the technical conditions under which the hearing took place. The document containing the record of the minutes shall be transmitted to the Attorney General to be forwarded to the requesting foreign authority.</p> <p>(11) The following shall mutatis mutandis apply to the person to be heard under the provisions of subarticle (6):</p> <p>(a) the provisions of article 522, where the person to be heard refuses to testify when required to do so by the magistrate;</p> <p>(b) the provisions of articles 104, 105, 107, 108 and 109, as the case may be, where the person to be heard does not testify to the truth, for this purpose the proceedings before the foreign authority shall be deemed to be proceedings taking place in Malta and the person to be heard shall be deemed to be a person testifying in those proceedings. For the purpose of determining the applicable punishment as may be necessary in proceedings for perjury under this subarticle the criminal fact being inquired into or adjudicated by the requesting foreign authority shall be deemed to be liable to the punishment to which it would have been liable had the same fact taken place in Malta or within the jurisdiction of the same Maltese criminal courts.</p> <p>(12) The provisions of subarticles (6) to (11), both inclusive, shall apply where the person to be heard is a person accused in the country of the requesting foreign authority provided that the hearing shall only take place with the consent of the person to be heard and that all the rules of evidence and procedure which would apply to the</p>	

Party	Legal provision and practical experience	Assessment
	<p>testimony of a person accused in criminal proceedings in Malta would also apply to the testimony of the person accused to be heard under this article.</p> <p>(13) The provisions of this article shall also apply mutatis mutandis where the request of the foreign authority is for the hearing of a witness or expert by telephone conference: provided that the witness or expert consents to the hearing.</p> <p>(14) Where the Attorney General has made a declaration as provided in subarticle (2), foreign officials designated by the foreign authority or international court which made the request shall be entitled to be present for the examination of witnesses or when investigative measures are being taken.</p> <p>435B. (1) Where the Attorney General receives a request made by a judicial, prosecuting or administrative authority of any place outside Malta or by an international court for investigations to take place in Malta in respect of a person (hereinafter in this article and in article 435BA referred to as "the suspect") suspected by that authority or court of a relevant offence, the Attorney General may apply to the Criminal Court for an investigation order or an attachment order or for both and the provisions of article 24A of the Dangerous Drugs Ordinance, hereinafter in this title referred to as "the Ordinance", shall mutatis mutandis apply to that application and to the suspect and to any investigation order or attachment order made by the court as a result of that application.</p> <p>(2) The phrase "investigation order" in subarticles (2) and (5) of the same article 24A of the Ordinance shall be read and construed as including an investigation order made under the provisions of this article.</p> <p>(3) The phrase "attachment order" in article 24A(6A) of the Ordinance shall be read and construed as including an attachment order under the provisions of this article.</p> <p>Chapter 164 of the Laws of Malta, The Police Act</p> <p>117. The Police may, directly or through regional or international police organisations, co-operate with any state agency having similar powers and duties in any other country.</p>	

Party	Legal provision and practical experience	Assessment
	<p>Subsidiary Legislation 440.05 Data Protection - (Processing of Personal Data in the Police Sector) Regulations.</p> <p>8. (1) The communication of personal data between different bodies exercising police powers shall only be permitted where there exists a legitimate interest for such communication within the framework of the legal powers of such bodies.</p> <p>(2) Communication of personal data from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties may only be made in accordance with regulation 10 if:</p> <p>(a) there exists a legal obligation or authorisation to communicate such data ; or (b) the Commissioner for Data Protection authorises such communication of data.</p> <p>(3) In exceptional cases, communication of personal data from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties, may also be made if:</p> <p>(a) it is clearly in the interest of the data subject and either the data subject himself has consented to the communication or circumstances are such as to allow a clear presumption of such consent; or (b) it is necessary for the prevention of a serious and imminent danger.</p> <p>(4) Bodies exercising police powers may also communicate personal data to other Government Departments or bodies established by law, if the data are necessary for the recipient to enable him to fulfil his lawful task and provided that the purpose of the processing to be performed by the recipient is not incompatible with the original processing or contrary to the legal obligations of the body exercising police powers.</p> <p>9. (1) Without prejudice to the provisions of any law or regulation laying down specific rules on the processing or exchange of personal data in the context of police and judicial cooperation, transfer of personal data to foreign authorities may only be made in accordance with regulation 10 and if the recipients of such data are bodies exercising police powers.</p> <p>(2) Subject to subregulation (1), such transfer of data shall only be permissible if there exists a legal obligation under any law, or an international obligation under a treaty,</p>	

Party	Legal provision and practical experience	Assessment
	<p>convention or international agreement on mutual assistance, to which Malta is a party.</p> <p>(3) In the absence of a provision as referred to in subregulation (2), transfer of data to foreign authorities may also be made if such communication is necessary for the prevention of a serious and imminent danger, or is necessary for the suppression of a serious criminal offence.</p> <p>10. (1) Requests for communication of personal data shall be submitted in writing to the body exercising police powers, and shall include an indication of the person or body making the request and of the reason and purpose for which the request is made unless any other law or any international agreement to which Malta is a party, provides otherwise.</p> <p>(2) The body exercising police powers shall reply in writing informing the body making the request of the decision taken as to whether the request can be met or not.</p> <p>(3) The body exercising police powers shall keep a record of all personal data communicated, indicating the following:</p> <p>(a) the details of the body making the request;</p> <p>(b) the purpose and reason for the request;</p> <p>(c) the date of transmission of data.</p> <p>(4) Personal data communicated from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties, or to foreign authorities, shall not be used for purposes other than those specified in the request for communication of data.</p> <p>(5) When it is necessary that personal data referred to in subregulation (4) be used for purposes other than those for which it was requested, the recipient shall submit a new request to the body exercising police powers in accordance with subregulation (1), and that data shall not be used by the recipient for purposes other than those included in the original</p>	
Panama	<p>The reply from Panama just refers to the Constitution of the Republic of Panama, the Judicial Code from Panama, the Penal Procedure Code and Law 51/2009. No specific legal framework respecting electronic evidence is in place.</p> <p>Moreover, it is mentioned that there is not in place any kind of agreement between</p>	<p>Article 17</p> <p>Panama is not in line with this Article.</p>

Party	Legal provision and practical experience	Assessment
	<p>police (or other public authority) and service providers or other that can store data, in the private sector.</p> <p>Regarding the process of preservation, it is described that, at the domestic level, after a complaint is received and the investigations start, a request has to be sent to the Corte Suprema de Justicia, in view of authorizing the interception of communications. This is the only way to obtain traffic data.</p> <p>In the Republic of Panama, the competence to execute international requests depends on the type of the procedure. Regarding computer crime, the competence belongs to the "Fiscalia Superior Especialidad en Delitos Contra la Propiedad Intelectual y Seguridad Informático".</p> <p>However, there are not in place any rules particularly applicable to the transfer of retained data to foreign authorities. The same rules that apply at the domestic level should apply at the international cooperation level.</p>	<p>Article 30</p> <p>Panama is not in line with this Article.</p> <p>The T-CY requests the authorities of Panama to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.</p>

5 Data preservation versus data retention

Party	Data retention regulations
1. Malta	<p>Regulation 19 of S.L. 440.01 states that a service provider of publicly available electronic communications services or of a public communications network shall retain the traffic data of its subscribers.</p> <p>The law is under review to align it with the requirements of the Decision of the Court of Justice of the European Union dated 8 April 2014, which declared the Directive 2006/24/EC invalid.</p> <p>The intention is to maintain the data retention law with some amendments.</p>
2. Panama	No information provided

6 Conclusions

Further to the assessments carried out in 2012⁵ and in June 2015⁶ the T-CY, at its 15th Plenary Session (24-25 May 2016) discussed and adopted the present report assessing the implementation by Malta and Panama of four articles of the Budapest Convention on Cybercrime:

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

6.1 Conclusions and recommendations

The T-CY,

- maintains that the assessment of the implementation of specific provisions of the Budapest Convention will enhance the effectiveness of this treaty;
- welcomes the replies to the T-CY questionnaire received from Malta and Panama.

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

1. The expedited preservation provisions of the Budapest Convention, in particular articles 16 and 29, are highly relevant tools to secure volatile evidence in an international context. The

⁵ [http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY\(2012\)10_Assess_report_v31_public.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/TCY2012/T-CY(2012)10_Assess_report_v31_public.pdf)

⁶ <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b>

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. Experience since 2012 suggests, indeed, that in the absence of specific domestic preservation powers, international requests for data preservation under Article 29 often require mutual legal assistance requests or a sufficient amount of information to support a domestic search, seizure or production order. In such situations, the preservation systems foreseen by the Convention on Cybercrime is not functional.
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.

6.2 Summary of implementation by Parties

Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)	Article 16 Expedited preservation	Article 29 Expedited preservation (international)	Article 17 Preservation and partial disclosure	Article 30 Preservation and partial disclosure (international)
1. Malta	Y	Y	N	N
2. Panama	P	N	N	N

6.3 Follow up

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

The T-CY will review progress made within 12 months of adoption of the report (that is, by mid-2017).

7 Appendix: Replies to questionnaire

7.1 Malta

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

1.1 Legislation/regulations

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

Chapter 9 of the Laws of Malta, Criminal Code

346. (1) It is the duty of the Police to preserve public order and peace, to prevent and to detect and investigate offences, to collect evidence, whether against or in favour of the person suspected of having committed that offence, and to bring the offenders, whether principals or accomplices, before the judicial authorities.

(2) Notwithstanding the generality of subarticle (1), where authorised by law and in the manner so provided, the Police may delay its immediate intervention for the prevention of the commission of an offence.

355AD. (1) Where, in the course of an investigation, a person attends voluntarily at, or accompanies a police officer to, a police station or office, that person shall be free to leave at any time, unless and until he is informed that he is under arrest.

(2) Where an inspector of Police has a reasonable suspicion that the person who attended voluntarily at the police station or office may have committed an offence subject to imprisonment, he may arrest such person forthwith without warrant and inform him accordingly. The time of the arrest shall be immediately recorded and immediate notice thereof shall be given to a Magistrate.

(3) The Police may, orally or by a notice in writing, require any person to attend at the police station or other place indicated by them to give such information and to produce such documents as the Police may require and if that person so attends at the police station or place indicated to him he shall be deemed to have attended that police station or other place voluntarily. The written notice referred to in this subarticle shall contain a warning of the consequences of failure to comply, as are mentioned in subarticle (5).

(4) Any person who is considered by the police to be in possession of any information or document relevant to any investigation has a legal obligation to comply with a request from the police to attend at a police station to give as required any such information or document:

Provided that no person is bound to supply any information or document which tends to incriminate him.

(5) A person who fails to comply with a notice in writing as is referred to in subarticle (3) or who fails, upon being so requested, even if only orally, to accompany voluntarily a police officer to a police station or other place indicated by the police officer for any purpose mentioned in the said subarticle (3) shall be guilty of a contravention punishable with detention and shall be liable to be arrested immediately under warrant.

(6) The notice mentioned in subarticle (3) may be served with urgency in cases where the interests of justice so require.

(7) A person who attends voluntarily as mentioned in subarticle (3) may be kept apart from any other person, but shall not be kept in any place normally used for the detention of arrested persons.

355E. (1) Saving the cases where the law provides otherwise, no police officer shall, without a warrant from a Magistrate, enter any premises, house, building or enclosure for the purpose of effecting any search therein or arresting any person who has committed or is reasonably suspected of having committed or of being about to commit any offence unless -

the offence is a crime other than a crime punishable under the Press Act and there is imminent danger that the said person may escape or that the *corpus delicti* or the means of proving the offence will be suppressed; or

.....

355H. No warrant of entry and search may be executed after sunset unless the Magistrate has otherwise authorised in the warrant, or unless the executing Police officer has reasonable cause to believe that the purpose of the entry and search will be frustrated if the execution of the warrant is delayed.

355Q. The Police may, in addition to the power of seizing a computer machine, require any information which is contained in a computer to be delivered in a form in which it can be taken away and in which it is visible and legible.

357. Where an officer of the Executive Police discovers any weapon, document, trace or vestige or any other thing relating to an offence, he shall take steps to establish and ensure the existence and the preservation thereof in the state in which it was found until he shall have reported the matter to the Court of Magistrates, and, if unable to establish and ensure such existence or preservation, he shall observe the same procedure provided for the drawing up of a "*repertus*".

558. (1) On the discovery of any document relating to any offence, steps shall be taken to secure the existence and preservation thereof, and a *procès-verbal*, to be known as "*repertus*", shall be drawn up.

(2) The expression "document" includes any paper and any material object which may furnish information, explanation, or other evidence about the offence, or about the guilt or innocence of the accused.

Subsidiary Legislation 440.01, PROCESSING OF PERSONAL DATA (ELECTRONIC COMMUNICATIONS SECTOR)

19. (1) Data retained under this Part shall be disclosed only to the Police or to the Security Service, as the case may be, where such data is required for the purpose of the investigation, detection or prosecution of serious crime.

(2) When data retained under this Part is required, such data shall be provided by a service provider of publicly available electronic communications services or of a public communications network, from whom it is required, in an intelligible form and in such a way that it is visible and legible.

(3) A request for data shall be made in writing and shall be clear and specific:

Provided that where the data is urgently required, such request may be made orally, so however that the written request shall be made at the earliest opportunity.

(4) Data retained under this Part shall, following the request, be provided without undue delay.

22. (1) The Police may, in addition to the request for data under regulation 19, issue a conservation order in relation to the data.

(2) The conservation order shall be served on the service provider within the retention period applicable under regulation 21.

(3) Where a conservation order has been issued, the service provider shall conserve the data -

(a) either for a period of six months in addition to the original or extended applicable retention period which period shall not, without an order of a Magistrate or of a competent Court, exceed a total period of two years; or

(b) where criminal proceedings have been commenced within the applicable retention period or within such period as extended in accordance with paragraph (a), for such time as may be necessary for the conclusion of the criminal proceedings where the data is required to be produced as evidence; such conclusion shall be deemed to occur when the judgement in the proceedings becomes final and conclusive, whichever is the longer period.

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

Yes, all types of data stipulated in article 16 are covered but provided that this data has in fact been stored in the computer system subject to the preservation/conservation order

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

Yes, they apply to electronic evidence in relation to any criminal offence

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

There are agreements between the Malta Police Force and the various service providers on the disclosure of data retained by the latter to the Police. These agreements are backed by legislation and Internal Police Directives.

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

While the preservation is not visible to the suspect or account holder automatically, there exists no possibility to prevent disclosure of the preservation request if a request for access is submitted by the data subject.

1.2 Procedures

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

Once a complaint is received by the police, verifications are immediately carried out in order to ascertain the existence of a criminal offence. Once the existence of an offence is ascertained, necessary investigations are conducted. All incoming requests are assessed by the Cybercrime Unit

Inspector who would then coordinate the technical assistance required for the investigation. Simultaneously, another Police Unit led by a Police Inspector would be in charge of conducting the overall investigation.

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

A standard template for requests is used.

1.3 Practical experience

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

Preservation/conservation orders are used very sporadically in Malta as it is specific to traffic data held by service providers, when compared to production orders or seizures pursuant to search warrants.

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

This information is not available to the respondent.

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

Conservation of traffic data is a specific legal measure provided for in Subsidiary Legislation 440.01. The Police generally uses seizure pursuant to the powers and obligations emanating from the Criminal Code.

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

No

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

Very good

Q 1.3.6 Please describe a typical case or scenario.

As per Q 1.2.1

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

The main strength of our system is that we have tools of general application which when coupled with the very good cooperation by the service providers yields good results.

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

1.4 Legislation/regulations

Q 1.4.1 What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

Vide under Q1.1.1 - there are no provisions related specifically to partial disclosure. The Police only request the data which is required for their investigations.

Q 1.4.2 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

Vide under Q.1.1.4

1.5 Procedures

Q 1.5.1 Please describe the end-to-end procedure for the handling of a request.

Vide under Q1.2.1

1.6 Practicalexperience

Q 1.6.1 How relevant to investigations in your country is partial disclosure?

Partial disclosure is widely used by the Police and this enables the controller to provide the relevant information earlier. Police requests are very specific usually requiring specific IP addresses, subscriber information, etc. This also makes it easier for the Police to handle the data in its possession.

Q 1.6.2 How frequently do you use these provisions?

These provisions are used on a daily basis.

Q 1.6.3 In general, what is the response time by service providers?

One week. In urgent cases, the response time is less (one day) as service providers would have been alerted about the request telephonically by the Police.

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

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

1.7 Legislation/regulations

Q 1.7.1 What legal provisions/regulations do you apply for executing an international request for preservation? Please list and attach text.

Chapter 9 of the Laws of Malta, Criminal Code

649. (1) Where the Attorney General communicates to a magistrate a request made by a judicial, prosecuting or administrative authority of any place outside Malta or by an international court for the examination of any witness present in Malta, or for any investigation, search or/and seizure, the magistrate shall examine on oath the said witness on the interrogatories forwarded by the said authority or court or otherwise, and shall take down the testimony in writing, or shall conduct the requested investigation, or order the search or/and seizure as requested, as the case may be. The order for search or/ and seizure shall be executed by the Police. The magistrate shall comply with the formalities and procedures indicated in the request of the foreign authority unless these are contrary to the public policy or the internal public law of Malta.

(2) The provisions of subarticle (1) shall only apply where the request by the foreign judicial, prosecuting or administrative authority or by the international court is made pursuant to, and in accordance with, any treaty, convention, agreement or understanding between Malta and the country, or between Malta and the court, from which the request emanates or which applies to both such countries or to which both such countries are a party or which applies to Malta and the said court or to which both Malta and the said court are a party. A declaration made by or under the authority of the Attorney General confirming that the request is made pursuant to, and in accordance with, such treaty, convention, agreement or understanding which makes provision for mutual assistance in criminal matters shall be conclusive evidence of the matters contained in that certificate. In the absence of such treaty, convention, agreement or understanding the provisions of subarticle (3) shall be applicable.

(3) Where the Minister responsible for justice communicates to a magistrate a request made by the judicial authority of any place outside Malta for the examination of any witness present in Malta, touching an offence cognizable by the courts of that place, the magistrate shall examine on oath the said witness on the interrogatories forwarded by the said authority or otherwise, notwithstanding that the accused be not present, and shall take down such testimony in writing.

(4) The magistrate shall transmit the deposition so taken, or the result of the investigation conducted, or the documents or things found or seized in execution of any order for search or/and seizure, to the Attorney General.

(5) For the purposes of subarticles (1) and (3) the magistrate shall, as nearly as may be, conduct the proceedings as if they were an inquiry relating to the *in genere* but shall comply with the formalities and procedures indicated by the requesting foreign authority unless they are contrary to the fundamental principles of Maltese law and shall have the same powers, or as nearly as may be, as are by law vested in the Court of Magistrates as court of criminal inquiry, as well as the powers, or as nearly as may be, as are by law conferred upon him in connection with an inquiry relating to the "*in genere*": provided that a magistrate may not arrest any person, for the purpose of giving effect to an order made or given under article 554(2), or upon reasonable suspicion that such person has committed an offence, unless the facts amounting to the offence which such person is accused or suspected to have committed amount also to an offence which may be prosecuted in Malta.

(5A) If the request cannot, or cannot fully, be executed in accordance with the formalities, procedures or deadlines indicated by the requesting foreign authority, the requesting authority shall be informed indicating the estimated time within which or the conditions under which execution of the request may be possible.

(5B) The proceedings referred to in this article shall, as nearly as may be, be conducted as if they were an inquiry relating to the "*in genere*".

(6) Where the request of the foreign authority is for the hearing of a witness or expert by video-conference, the provisions of subarticles (7) to (12), both inclusive, shall apply.

(7) The magistrate shall summon the person to be heard to appear at the time and place equipped with videoconference facilities appointed for the purpose by the magistrate. The magistrate shall give effect to any measures for the protection of the person to be heard which the Attorney General may declare to have been agreed upon with the requesting foreign authority.

(8) The magistrate shall conduct the hearing and where necessary the magistrate shall appoint an interpreter to assist during the hearing. The magistrate present shall ensure that the person to be heard is identified and that the proceedings take place and continue at all times in conformity with the fundamental principles of the law of Malta.

(9) The person to be heard may claim the right not to testify which would accrue to him or her under the law of Malta or under the law of the country of the requesting foreign authority.

(10) Subject to any measures for the protection of the person to be heard referred to in subarticle (7), the magistrate shall on the conclusion of the hearing draw up minutes indicating the date and place of the hearing, the identity of the person heard, the identities and functions of all other persons participating in the hearing, any oaths taken and the technical conditions under which the hearing took place. The document containing the record of the minutes shall be transmitted to the Attorney General to be forwarded to the requesting foreign authority.

(11) The following shall *mutatis mutandis* apply to the person to be heard under the provisions of subarticle (6):

(a) the provisions of article 522, where the person to be heard refuses to testify when required to do so by the magistrate;

(b) the provisions of articles 104, 105, 107, 108 and 109, as the case may be, where the person to be heard does not testify to the truth, for this purpose the proceedings before the foreign authority shall be deemed to be proceedings taking place in Malta and the person to be heard shall be deemed to be a person testifying in those proceedings. For the purpose of determining the applicable punishment as may be necessary in proceedings for perjury under this subarticle the criminal fact being inquired into or adjudicated by the requesting foreign authority shall be deemed to be liable to the punishment to which it would have been liable had the same fact taken place in Malta or within the jurisdiction of the same Maltese criminal courts.

(12) The provisions of subarticles (6) to (11), both inclusive, shall apply where the person to be heard is a person accused in the country of the requesting foreign authority provided that the hearing shall only take place with the consent of the person to be heard and that all the rules of evidence and procedure which would apply to the testimony of a person accused in criminal proceedings in Malta would also apply to the testimony of the person accused to be heard under this article.

(13) The provisions of this article shall also apply *mutatis mutandis* where the request of the foreign authority is for the hearing of a witness or expert by telephone conference: provided that the witness or expert consents to the hearing.

(14) Where the Attorney General has made a declaration as provided in subarticle (2), foreign officials designated by the foreign authority or international court which made the request shall be entitled to be present for the examination of witnesses or when investigative measures are being taken.

435B. (1) Where the Attorney General receives a request made by a judicial, prosecuting or administrative authority of any place outside Malta or by an international court for investigations to take place in Malta in respect of a person (hereinafter in this article and in article 435BA referred to as

"the suspect") suspected by that authority or court of a relevant offence, the Attorney General may apply to the Criminal Court for an investigation order or an attachment order or for both and the provisions of article 24A of the Dangerous Drugs Ordinance, hereinafter in this title referred to as "the Ordinance", shall *mutatis mutandis* apply to that application and to the suspect and to any investigation order or attachment order made by the court as a result of that application.

(2) The phrase "investigation order" in subarticles (2) and (5) of the same article 24A of the Ordinance shall be read and construed as including an investigation order made under the provisions of this article.

(3) The phrase "attachment order" in article 24A(6A) of the Ordinance shall be read and construed as including an attachment order under the provisions of this article.

Chapter 164 of the Laws of Malta, The Police Act

117. The Police may, directly or through regional or international police organisations, co-operate with any state agency having similar powers and duties in any other country.

Subsidiary Legislation 440.05 Data Protection - (Processing of Personal Data in the Police Sector) Regulations.

8. (1) The communication of personal data between different bodies exercising police powers shall only be permitted where there exists a legitimate interest for such communication within the framework of the legal powers of such bodies.

(2) Communication of personal data from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties may only be made in accordance with regulation 10 if:

(a) there exists a legal obligation or authorisation to communicate such data ; or

(b) the Commissioner for Data Protection authorises such communication of data.

(3) In exceptional cases, communication of personal data from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties, may also be made if:

(a) it is clearly in the interest of the data subject and either the data subject himself has consented to the communication or circumstances are such as to allow a clear presumption of such consent; or

(b) it is necessary for the prevention of a serious and imminent danger.

(4) Bodies exercising police powers may also communicate personal data to other Government Departments or bodies established by law, if the data are necessary for the recipient to enable him to fulfil his lawful task and provided that the purpose of the processing to be performed by the recipient is not incompatible with the original processing or contrary to the legal obligations of the body exercising police powers.

9. (1) Without prejudice to the provisions of any law or regulation laying down specific rules on the processing or exchange of personal data in the context of police and judicial cooperation, transfer of personal data to foreign authorities may only be made in accordance with regulation 10 and if the recipients of such data are bodies exercising police powers.

(2) Subject to subregulation (1), such transfer of data shall only be permissible if there exists a legal obligation under any law, or an international obligation under a treaty, convention or international agreement on mutual assistance, to which Malta is a party.

(3) In the absence of a provision as referred to in subregulation (2), transfer of data to foreign authorities may also be made if such communication is necessary for the prevention of a serious and imminent danger, or is necessary for the suppression of a serious criminal offence.

10. (1) Requests for communication of personal data shall be submitted in writing to the body exercising police powers, and shall include an indication of the person or body making the request and of the reason and purpose for which the request is made unless any other law or any international agreement to which Malta is a party, provides otherwise.

(2) The body exercising police powers shall reply in writing informing the body making the request of the decision taken as to whether the request can be met or not.

(3) The body exercising police powers shall keep a record of all personal data communicated, indicating the following:

(a) the details of the body making the request;

(b) the purpose and reason for the request;

(c) the date of transmission of data.

(4) Personal data communicated from bodies exercising police powers, to other Government Departments or to bodies established by law, or to other private parties, or to foreign authorities, shall not be used for purposes other than those specified in the request for communication of data.

(5) When it is necessary that personal data referred to in subregulation (4) be used for purposes other than those for which it was requested, the recipient shall submit a new request to the body exercising police powers in accordance with subregulation (1), and that data shall not be used by the recipient for purposes other than those included in the original request unless there is written agreement to the new request.

Q 1.7.2 Who has the competence for receiving and executing the international preservation request? What is the role of the contact point?

The Office of the Attorney General is the Central Designated Authority in relation to requests for Mutual Legal Assistance in Criminal Matters in terms of article 649 of the Criminal Code. The role of the Attorney General is explained in the article itself.

The Police have a role in relation to requests for police cooperation and requests for mutual legal assistance (MLA). The role of the Police in relation to MLA requests is defined in article 649 of the Criminal Code. The role of the Police in relation to requests for police cooperation is provided for in article 117 of the Police act and is generally related to the preservation and exchange of information.

The relevant contact points within the Police are the Cybercrime Unit in relation to requests pursuant to the Cybercrime Convention and the International Relations Unit in relation to requests for police cooperation in terms of the Europol Decision or the ICPO agreement or any bilateral agreement.

Q 1.7.3 What rules apply for the transfer of the data preserved to foreign authorities?

Data preserved in terms of article 29 of the Cybercrime Convention are only transferred to foreign authorities in terms of a request for MLA or in terms of articles 9 and 10 of Subsidiary legislation 4401.05.

1.8 Procedures

Q 1.8.1 Please describe the end-to-end procedure for the handling of the request.

Upon receipt of a request, action is taken in accordance with the legal basis under which the request is made. Requests may be received either via police cooperation services, the cybercrime contact point, the Office of the Attorney General or Eurojust.

Q 1.8.2 What templates/forms are used for international requests? Please attach if any.

The use of templates may be required only in certain instances. Requests sent via Europol channels are channeled via the SIENA application and all requests would be structured accordingly. Requests sent via ICPO channels do not generally require a specific format. No template is used by the Cybercrime Unit when sending requests via their channels. Requests sent via MLA channels use the jargon and forms appropriate for MLA requests (vide for example the compendium made available by the EJM at http://ejn-crimjust.europa.eu/ejm/EJM_Compendium.aspx or the MLA tool made available by UNODC at http://www.unodc.org/mla/en/download_MLA_Tool.html)

Q 1.8.3 Other than the information listed in Article 29.2, what information do you need in order to execute a request?

The information mentioned in article 29.2 are sufficient for execution

1.9 Practical experience

Q 1.9.1 How frequently do you send and receive international preservation requests? Please provide estimated numbers if readily available.

Rarely

Q 1.9.2 In general, as a requested country, how quickly do you issue a preservation request?

Generally, these are issued within few days from when the need for such request is identified.

Q 1.9.3 In general, as a requesting country, how quickly are you notified that your request has been issued in the foreign country?

Information is not available

Q 1.9.4 Please describe a typical case or scenario.

As per Q 2.5.2

Q 1.9.5 Without provisions on preservation, would this create problems for international cooperation?

This depends on the State from where the preservation is requested.

Q 1.9.6 How often are international preservation requests that you receive not followed by mutual legal assistance requests?

An MLA followed in most cases we had

Q 1.9.7 How often do you send international preservation requests and not follow them with mutual legal assistance requests or notifications?

Our requests for preservation would generally be followed by an MLA request. When this is not the case, a formal request for police cooperation is sent via Europol or Interpol channels

Q 1.9.8 In conclusion: What are the main strengths and what are the main problems of preservation within the framework of international cooperation?

Lack of acknowledgement or receipt or no reply whatsoever from the requested State are the main problems which we encounter.

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

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

1.10 Legislation/regulations

Q 1.10.1 What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

Vide under Q.2.4.1

Q 1.10.2 What are the conditions, limitations or impediments to disclosing a sufficient amount of traffic data?

The conditions, limitations or impediments are those indicated in the applicable legal provisions. Vide under Q2.4.1.

1.11 Procedures

Q 1.11.1 Please describe the end-to-end procedure for the handling of a request.

Vide under Q 2.4.2

1.12 Practicalexperience

Q 1.12.1 How frequently do you use this provision?

Rarely

Q 1.12.2 Please describe a typical case or scenario.

Upon receipt of a request for assistance from foreign authorities a written request is drawn up and dispatched to the local service provider. The information requested by the foreign authorities is either preserved by the service provider or collected by the Malta Police (if the information would require further investigations). The information will be disclosed to the foreign authorities upon receipt of a formal request received either via police channels (Europol) or judicial authorities.

Q 1.12.3 Without provisions on partial disclosure, would this create problems for international cooperation?

Vide Q 2.6.5.

7.2 Panama

1. Artículo 16 – Conservación Rápida de Datos Informáticos Almacenados (nivel nacional)

1.1 Legislación/regulaciones

P.1.1.1. ¿Qué disposiciones legales se aplican? Por favor enumere y adjunte el texto. Por favor también describa y adjunte reglamentos o regulaciones de aplicación interno (si las hubiere).

En la República de Panamá, existen estas normas:

- Código Penal de la República de Panamá (Artículos 289, 290, 291 y 292). [Existe Proyecto de Ley para Modificación y Adición de nuevos artículos].
- Ley 23 de 1986 (Delitos Relacionados con Drogas [Artículo 46: Centro Nacional de Informática Policial].
- Ley 42 de 2000 (Medidas para Prevención de Blanqueo de Capitales [Análisis de Bases de Datos para Prevención de Blanqueo – Genérica-].
- Ley 06 de 2002 (Normas de Transparencia de Gestión Pública [Información Confidencial, Gubernamental e Información de Acceso Libre].
- Ley 16 de 2004 (Prevención de Explotación Sexual incluye menores y adolescentes) [Intervención de Base de Datos].
- Ley 15 de 2008 (Medidas de Informatización de los Proceso Judiciales).
- Ley 51 de 2008 (Ley de Documentos Electrónicos, Almacenamiento y Comercio Electrónico)
- Ley 51 de 2009 (Ley de Conservación, Protección y Suministro de Datos de Usuarios de los Servicios de Telecomunicaciones)
- Ley 82 de 2012 (Ley de Firma Electrónica)
- Ley 83 de 2012 (Uso de Medio Electrónicos para trámites gubernamentales).
- Ley 121 de 2013 (Reforma el Código Penal [Sección 5ª, Interceptación de Comunicaciones e incautación de Datos].

P.1.1.2. ¿Cubren todos los tipos de datos (tráfico, contenido) estipulados en el artículo 16?

Existen Normas que cubren algunos tipos de datos (Base de datos, firma electrónica, factura electrónica, certificado electrónico).

no se ha aprobado hasta el momento el manual de manejo de evidencia digital.

1.3 Experiencia práctica

P.1.3.1. ¿Qué tan relevante para las investigaciones en su país se agiliza la conservación? ¿Qué tan relevante se agiliza la conservación en comparación a otras medidas (orden de producción, búsqueda y captura)?

Es importante en nuestro país, ya que es una parte fundamental en la que se obtendrá la evidencia, para poder llevar a juicio a los presuntos responsables.

P.1.3.2. ¿Con qué frecuencia utiliza estas disposiciones? De estar disponible, por favor proporcione el número estimado de solicitudes.

No tenemos una cifra concreta en este tema, ya que otras agencias también realizan este tipo de diligencias.

P.1.3.3. ¿En su país, es la conservación una medida prevista específicamente en el derecho procesal, o debe usted ordenar conservación a través de inspección/registro, orden de exhibición u otros poderes?

En nuestro país, la medida de conservación no está taxativamente establecida en nuestro derecho procesal, es implícita cuando los códigos judicial, procesal penal, civil, comercial; establecen las pruebas lícitas y establecen las formas de recuperación y adquisición de evidencias, que deben ser dispuestas mediante resolución de inspección ocular o allanamiento y registro.

P.1.3.4. ¿Se hace entrega de citaciones de solicitudes de conservación a personas naturales o jurídicas además de hacerlo a los proveedores de servicios?

En nuestro país, no se aplica estas medidas a las personas naturales. En cuanto a los proveedores de servicios sí están obligados a la conservación, que está estipulado en la Ley 51 de 2009.

2. Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico.

2.1. Legislación/regulaciones

P.2.1.1. ¿Qué disposiciones legales se aplican? Por favor enumere y adjunte el texto. Por favor también describa y adjunte reglamentos o regulaciones de aplicación interno (si las hubiere).

- Constitución de la República de Panamá
- Código Judicial de Panamá
- Código Procesal Penal
- Ley 51 de 2009

P.2.1.2. ¿Qué acuerdos o arreglos voluntarios existen entre la policía y los proveedores de servicio u otros titulares o tenedores de datos del sector privado?

En la República de Panamá, no existe ningún acuerdo entre la policía, los proveedores de servicios o titulares o tenedores de datos del sector privado.

2.2 Procedimientos

P.2.2.1. Por favor describa el procedimiento de extremo a extremo para el manejo de una solicitud.

- A. Recepción de la denuncia
- B. Inicio de la Investigaciones
- C. Cabeza de Proceso
- D. Solicitud de permiso a la Corte Suprema de Justicia, para aval de interceptación de datos en tránsito
- E. Otorgada el permiso se procede a realizar las interceptaciones correspondientes, que deben ser a su vez establecida mediante resolución motivada junto con el permiso ya otorgado por parte de la Corte Suprema de Justicia.

mecanismos como, el principio de reciprocidad y la membresía de interpol.

P.3.1.2. ¿Quién tiene la competencia de recibir y ejecutar solicitudes internacionales de conservación? ¿Qué papel desempeña el punto de contacto?

En la república de Panamá quienes tienen competencia dependerá del tipo de proceso. En lo que respecta a delitos informáticos tendrá competencia primaria Fiscalía Superior Especialidad en delitos Contra la Propiedad Intelectual y Seguridad Informático, y luego de ejecutada la asistencia internacional se procede a trasladar la documentación a la Fiscalía de Asuntos Internacionales, y posteriormente a el Ministerio de Relaciones Exteriores, para que sea enviado a la autoridad requirente.

P.3.1.3. ¿Qué reglas se aplican para la transferencia de los datos conservados a autoridades extranjeras?

Para solicitudes internacionales, se aplica igual que las mismas reglas que se utiliza a lo interno.

3.2 Procedimientos

P.3.2.1. Por favor describa el procedimiento de extremo a extremo para el manejo de la solicitud

A. Receptación de la Solicitud de Asistencia Legal

B. Inicio de la Investigaciones

C. Cabeza de Proceso

D. De ser necesario se realiza la solicitud de permiso a la Corte Suprema de Justicia, para aval de interceptación de datos en tránsito

E. Otorgada el permiso se procede a realizar las interceptaciones correspondientes, que deben ser a su vez establecida mediante resolución motivada junto con el permiso ya otorgado por parte de la Corte Suprema de Justicia.

F. Todas las diligencias para esclarecer todo lo solicitado, finalizada la investigación,

F. Se envía por el conducto de la Fiscalía de Asuntos Internacionales, y quienes deberán enviarlo al Ministerio de Relaciones Exteriores, y a su vez remitirlo a la autoridad requirente.

P.3.3.4. Por favor describa un caso típico o escenario.

P.3.3.5. Sin disposiciones en conservación, causaría esto problemas para la cooperación internacional?