COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/TCY

Strasbourg, version 21 June 2015 T-CY (2015)6

Cybercrime Convention Committee (T-CY)

Assessment report

Implementation of the preservation provisions of the Budapest Convention on Cybercrime

Supplementary report

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

Contents

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 present report provides a draft assessment of these Parties to the extent that they have provided replies to the questionnaire.

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

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:[2]

- 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?

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

[2] 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

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"[3] 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 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] Page 77ff.

3 Implementation of Articles 16 and 29 on expedited preservation

Party	Legal provisions and practical experience	T-CY Assessment
1. Australia	Article 16 – Domestic procedures Divisions 1 and 2 of Part 3-1A of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) establish a legal regime that allows Australian enforcement agencies and the Australian Security Intelligence Organisation (the Organisation) to require carriers (and carriage service providers) to preserve the content of 'stored communications', as well as traffic data associated with those stored communications. The procedure involves: Preservation Step 1 — Request by agency to carrier (section 107H, TIA Act) Step 2 — End of preservation notice (sections 107K and 107L, TIA Act) Access Step 1 — Application to issuing officer (section 110, TIA Act) Step 2 — Consideration of application for warrant (section 116, TIA Act) Step 3 — Use of stored communications warrant (section 117, TIA Act) Australian preservation notices only cover content and traffic data that is associated with 'stored communications'. Australian preservation notices are not available for traffic data associated with other types of communications. The reason why Australian preservation notices do not cover other types of traffic data is that the legal regime for *access* to traffic data allows enforcement agencies to access traffic data in a timely fashion when it is required for an investigation. As such, the Australian Government considers that it is unnecessary to implement a separate preservation notice regime for traffic data. The preservation notice regime under Divisions 1 and 2 of Part 3-1A of the TIA Act applies only to carriers and carriage service providers. As explained in our response to question 1.1.4, Australian enforcement agencies may	Article 16 Australia is partially in line with this Article. Article 29 Australia is partially in line with this Article. The T-CY requests the authorities of Australia to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.

Party	Legal provisions and practical experience	T-CY Assessment
	request that other physical or legal persons preserve data, however they do not have the power to compel other physical or legal persons to preserve data. Information on the actual use of these provisions was not provided. [4] <u>Article 29 – International preservation requests</u> Under section 107P of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), a foreign country can make a request to the Australian Federal Police (AFP) to arrange for the preservation of certain stored communications if that country intends to make a formal mutual assistance request to access those communications. Upon receiving a request from a foreign country, the AFP must give the carrier a written notice requiring the carrier to preserve all stored communications relevant to the person or telecommunications service in question that is held by the carrier at any time between when it receives the request and the end of that day. In addition to the requirements at paragraph 107P(1)(a) and 107P(b), paragraph 107P(1)(c) of the TIA Act requires the communications to be relevant to an investigation, or investigative proceeding, relating to a criminal matter involving a 'serious foreign contravention'. Section 5EA of the TIA Act defines 'serious foreign contravention' as a contravention of a law of a foreign country that is punishable by a maximum penalty of: (a) imprisonment for 3 years or more, imprisonment for life or the death – penalty; or (b) a fine of an amount that is at least equivalent to 900 penalty units (that is, A$153,000). The procedure involves: Preservation Step 1 — Request by foreign country to AFP (section 107P, TIA Act)	

[4] See Annual Reports on the use of powers under the TIA http://www.ag.gov.au/NationalSecurity/TelecommunicationsSurveillance/Pages/Annualreports.aspx

Party	Legal provisions and practical experience	T-CY Assessment
	Step 2 — Request by AFP to carrier (section 107N, TIA Act) Step 3 — End of preservation notice (sections 107Q and 107R, TIA Act) Access Step 1 — Request by foreign country Step 2 — Attorney-General authorisation (section 15B, MA Act) Step 3 — Application to issuing officer (section 110, TIA Act) Step 4 — Consideration of application for warrant (section 116, TIA Act) Step 5 — Use of stored communications warrant (section 117, TIA Act) Step 6 — Provision of material to foreign country (sections 139, 142 and 142A, TIA Act) In 2012-13, the Australian Federal Police did not issue any foreign preservation notices. (More recent data is not yet available).	
2. Austria	In the absence of specific preservation powers, other provisions of the Criminal Procedure Code are used to secure data, including seizure (§ 110 and 111), search (§119 – 122), "confiscation of information about data of a message transmission" (§135) as well as common provisions (§138). No information has been provided on the actual use of these provisions for preservation purposes.	Article 16 Austria does not have specific powers to order or similarly obtain the expeditious preservation of specified computer data. Austria is therefore not in line with this Article. Article 29 Austria is not in line with this Article The T-CY requests the authorities of Austria to undertake the necessary reforms to bring domestic regulations and practices in

Party	Legal provisions and practical experience	T-CY Assessment
		line with the Budapest Convention on Cybercrime.
3. Belgium	Belgium does not yet have any legislation transposing the articles 16 and 17 of the convention into Belgian law. There is currently work on a legislative proposal to do so. Seizure powers (article 39bis CPC) are used in the meantime to secure data.	Article 16 While reforms are envisaged, Belgium is currently not in line with this Article. Article 29 While reforms are envisaged, Belgium is currently not in line with this Article. The T-CY requests the authorities of Belgium to complete the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.
4. Czech Republic	In the absence of specific preservation provisions, – Production orders under Section 78 of the Criminal Procedure Code is used for traffic and location data; – The general provision of Section 8 of the Criminal Procedure Code *((1) State authorities, legal entities and natural persons are obliged without needless delay and also, unless stipulated otherwise in a special regulation, without payment, to comply with requests from law enforcement bodies in performance of their duties.*) is used for other data. For international requests, an MLA request is necessary.	Article 16 The Czech Republic is partially in line with this Article. Article 29 The Czech Republic is not in line with this Article. The T-CY requests the authorities of the

Party	Legal provisions and practical experience	T-CY Assessment
	Information provided by Czech's authorities regarding the draft assessment: Comments sent by the Czech Republic on 11 June 2015: A) Article 16 Expedited preservation of stored computer data It is true that there are indeed no specific legal provisions on expedited preservation in the Czech legal order at the present time. Nevertheless general powers regarding traffic and location data can be used when conditions under Code of Criminal Procedure are met. Moreover the fact that traffic data can be expeditiously obtained through general powers is confirmed also in Assessment report on Czech Republic sent to us, page 8. In general the Assessment report on page 4 states: "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". We would like to have an explanation which restrictions we have in our laws so that we are not in line with art. 16 (concerning traffic and location data). Moreover, the explanatory report for the Budapest Convention concerning Art. 16 stated as follows: "The article does not specify how data should be preserved. It is left to each Party to determine the appropriate manner of preservation and whether, in some appropriate cases, preservation of the data should also entail its 'freezing'. The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or	Czech Republic to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.

Party	Legal provisions and practical experience	T-CY Assessment
	administrative order or directive (e.g. from police or prosecutor). In some States, preservation orders do not exist in their procedural law, and data can only be preserved and obtained through search and seizure or production order. Flexibility is intended by the use of the phrase 'or otherwise obtain' to permit these States to implement this article by the use of these means." Provided the flexibility given to Parties in explanatory report concerning this article, we believe we are partially in line with article 16.	
5. Denmark	"The Administration of Justice Act Section 786a" provides for powers to order the preservation of any data by providers: "The Administration of Justice Act Section 786a. (1) In connection with an investigation in which electronic evidence may be of importance, the police may impose orders on providers of telecom networks or services to arrange for emergency protection of electronic data, including traffic data. (2) An order of emergency protection under subsection (1) above may solely comprise electronic data stored at the point in time when the order is imposed. The order must state the data that must be secured and the period for which they must be secured (the period of protection). The order must be limited to comprise solely the data estimated to be necessary for investigation and the protection period must be as short as possible and no more than 90 days. An order of this nature may not be extended. (3) Providers of telecom networks or services are responsible for ensuring as part of the protection under subsection (1) without undue delay that they pass on traffic data concerning other telecom network or service providers whose networks or services have been used in connection with the electronic communication that may be of importance for the investigation. (4) Violation of subsections (1) and (3) above is punishable by a fine." According to clarifications provided by Denmark,	Article 16 Denmark is in line with this Article. Article 29 Denmark is partially in line with this Article.

Party	Legal provisions and practical experience	T-CY Assessment
	– Section 786a of the Danish Administration of Justice Act applies to "providers of telecom networks or services" and covers all internet providers and telecommunication companies. The provision thus enables the police to impose orders of emergency protection on businesses that – as part of their economic activities – provide internet- or telecommunication services and thereby retain electronic data which can be relevant to the police's investigation. – Furthermore, section 786 a should be read in conjunction with other relevant provisions of the Administration of Justice Act, inter alia section 804 (on discovery) which enables the police to secure evidence – including electronic data – retained by persons who are not suspects, e.g. banks, employers or other physical or legal persons. The power seems to be rarely used in domestic proceedings, but is used for international requests. According to clarifications provided by Denmark, "there is no specific Danish legislation concerning mutual legal assistance in criminal matters. In all cases where mutual legal assistance from Denmark is required the Danish authorities apply national legislation by analogy. This implies that the Danish authorities can comply with a request for mutual legal assistance if the investigative measures covered by the request could be carried out in a similar national case, e.g. in accordance with the above mentioned sections 786a and 804 of the Administration of Justice Act." International preservation requests may be sent through the 24/7 point of contact.	
6. Dominican Republic	Preservation powers are specifically foreseen by law 53-07 on cybercrime: Artículo 53.- Conservación de los Datos. Las autoridades competentes actuarán con la celeridad requerida para conservar los datos contenidos en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.	Article 16 The Dominican Republic is in line with this Article.

Party	Legal provisions and practical experience	T-CY Assessment
	Artículo 54.- Facultades del Ministerio Público. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: b) Ordenar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos; It is rarely used to order preservation from domestic providers but more often with regard to international requests. At the domestic level, search, seizure and production orders used directly.	Article 29 Dominican Republic is in line with this Article.
7. Iceland	Preservation powers are provided for in Paragraph 47 of the Communications Act 81/2003: *Í þágu rannsóknar máls er lögreglu heimilt að leggja fyrir fjarskiptafyrirtæki að varðveita þegar í stað tölvugögn, þar með talin gögn um tölvusamskipti. Fyrirmæli lögreglu geta eingöngu tekið til gagna sem þegar eru fyrir hendi. Í fyrirmælunum á að koma fram hvaða gögn eigi að varðveita og hve lengi, en sá tími má þó ekki vera lengri en 90 dagar.* Unofficial English translation: The police may in the process of an investigation order a telecommunication company to preserve immediately computer data, including traffic data. The order of the police may only apply to already existing data. The order shall prescribe which data to preserve and for how long, this time may, however, not exceed 90 days.	Article 16 Iceland is partially in line with this Article. There is no specific provision for expedited preservation for electronic data that are not traffic data. Non-traffic data may be preserved by use of general powers for freezing and seizing data in criminal matters.

Party	Legal provisions and practical experience	T-CY Assessment
	In practice, a request would be sent to the police in the respective district, which in turn would contact the service provider(s). If, however, the request would involve a serious incident such as an act of terrorism, then the request would be dealt with by the National Commissioner of the Police. Preservation is rarely used in domestic proceedings, but seizure is applied directly. According to clarifications provided by Iceland: "In the newly adopted (April 2015) cyber security policy for Iceland, review and revision of the legal framework relating to cybercrime is one of the main actions (Action 15). Review of compliance with Article 16 and 29 is one of the points identified. Until the review has been completed and possible revisions made, it cannot be asserted that Iceland is in full compliance with the Articles 16 and 29."	Article 29 Iceland is partially in line with this Article, as there is no specific provision for expedited preservation for electronic data that are not traffic data. Preservation of non-traffic data would require an MLA request. The T-CY requests the authorities of Iceland to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.
8. Japan	Preservation powers are foreseen in: – Art. 218 (search and seizure) and Art. 197(3) (preservation request) of the Code of Criminal Procedure with respect to Art. 16(1) of the Convention – Art. 197(3) (preservation request) and Art. 197(4) (extension of preservation period) of the Code of Criminal Procedure with respect to Art. 16(2) of the Convention – Art. 197(5) (request for confidentiality) of the Code of Criminal Procedure with respect to Art. 16(3) of the Convention With respect to some service providers, the Police apply the procedure specified by respective providers, such as pre-notification of seizure of computer data. The procedure involves: (1) Investigating authorities specify the computer data necessary for investigation and the holder(s) of such data.	Article 16 Japan 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. Article 29 Japan is in line with this Article.

Party	Legal provisions and practical experience	T-CY Assessment
	(2) Public prosecutor, public prosecutor's assistant officer or a judicial police official (hereinafter referred to as "investigating officials") drafts the preservation request document and sends it to the data holder [for traffic data only]. (3) Investigating officials request for issuance of a seizure warrant to a judge and receive the warrant. (4) Investigating officials show the seizure warrant to the data holder (service provider) and seize the data specified in the warrant upon submission by the holder. In Japan, preservation of traffic data is done expeditiously pursuant to Art. 197 of the Code of Criminal Procedure. A preservation request pursuant to Art. 197 may be carried out without a warrant issued by a judge, unlike a search or a seizure. In Japan, preservation of computer data other than traffic data is done through seizure promptly upon issuance of a warrant by a judge pursuant to Art. 218 of the Code of Criminal Procedure. Since the Japanese judges usually issue a seizure warrant in 1 day, the requirement for a warrant has not posed any obstacles to an investigation up until now. In 2013, some 230 requests for the preservation of traffic data were issued. For international requests (Article 29 Budapest Convention), the following provisions are used: – Art. 3, Art. 5, Art. 8(1)vi and Art. 8(2) of the Act on International Assistance in Investigation and Other Related Matters – Art. 197(3) of the Code of Criminal Procedure Requests based on the Budapest Convention can be received by the 24/7 point of contact, that is, the National Public Safety Commission (the National Police Agency). In 2013, sent 124 preservation requests through Interpol channels and 40 through the G8 24/7 network.	

Party	Legal provisions and practical experience	T-CY Assessment
9. Malta	No information received	The T-CY regrets that no information has been received and recalls that under the Rules of Procedure, "T-CY members shall participate in the assessment of the implementation of the Convention".
10. Mauritius	Mauritius, through the Computer Misuse and Cybercrime Act 2003, introduced legal provisions for the expedited preservation of stored data. Section 11 of the Act (reproduced below) stipulates that an investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data. *11. Preservation order* *(1) Any investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.* *(2) For the purposes of subsection (1), data includes traffic data and subscriber information.* *(3) An order made under subsection (1) shall remain in force—* *(a) until such time as may reasonably be required for the investigation of an offence;* *(b) where prosecution is instituted, until the final determination of the case; or* *(c) until such time as the Judge in Chambers deems fit.* In its interpretation section *"data"* is defined as follows: *"data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium.*	<u>Article 16</u> Mauritius is in line with this Article. <u>Article 29</u> Mauritius is not in line with this provision since MLA requests are required. The T-CY requests the authorities of Mauritius to complete the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.

Party	Legal provisions and practical experience	T-CY Assessment
	The term investigatory authority has been defined in the Act as *"the police or any other body lawfully empowered to investigate any offence".* Mauritius has so far not received nor sent preservation requests to other countries.	
11. Panama	No information received	The T-CY regrets that no information has been received and recalls that under the Rules of Procedure, "T-CY members shall participate in the assessment of the implementation of the Convention".

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

Party	Legal provision and practical experience	Assessment
1. Australia	Article 17 – domestic procedure Australian preservation notices only cover content and traffic data that is associated with 'stored communications'. Australian preservation notices are not available for traffic data associated with other types of communications. The power to partially disclose traffic data is not foreseen in the law and thus disclosure by a provider would constitute a criminal offence. However, a person may be authorized to voluntarily disclose data needed in a criminal investigation (Article 177 ff TIA Act). Article 30 – international procedure Under section 180A of the TIA Act, after receiving a request from a foreign country, an authorised officer of the AFP may authorise a carrier or carriage service provide to disclose to the AFP preserved traffic data where the officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country. Following receipt of the preserved traffic data, the officer can authorise the disclosure of the data to a foreign law enforcement agency if satisfied of certain criteria (sections 180A and 180F, TIA Act). A person must not disclose preserved traffic data to a foreign law enforcement agency unless the disclosure is subject to the following conditions: – that the information will only be used for the purposes for which the foreign country requested it, and – the information will be destroyed where it is no longer required.	Article 17 Australia is in line with this Article. Article 30: Australia is in line with this Article.

Party	Legal provision and practical experience	Assessment
2. Austria	In the absence of specific preservation provisions other powers are used. It is unclear whether they would allow for partial disclosure of traffic data.	Article 17 Austria is not in line with this Article. Article 30 Austria is not in line with this Article. The T-CY requests the authorities of Austria to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.
3. Belgium	Pending reform of the legislation, seizure powers are used to secure data also upon international requests.	Article 17 While reforms are envisaged, Belgium is currently not in line with this Article. Article 30 While reforms are envisaged, Belgium is currently not in line with this Article. The T-CY requests the authorities of Belgium to complete the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on

Party	Legal provision and practical experience	Assessment
		Cybercrime.
4. Czech Republic	In the absence of specific preservation provisions, – Production orders under Section 78 of the Criminal Procedure Code is used for traffic and location data; – The general provision of Section 8 of the Criminal Procedure Code (*(1) State authorities, legal entities and natural persons are obliged without needless delay and also, unless stipulated otherwise in a special regulation, without payment, to comply with requests from law enforcement bodies in performance of their duties*.) is used for other data. For international requests, a MLA request is necessary. After receiving the draft assessment the Czech authorities replied on 11 June 2015: B) Article 17 Expedited preservation and partial disclosure of traffic data Unfortunately the Act No. 127/2015 on electronic communications was not mentioned in our questionnaire. Section 97 para. 3 of this act stipulates as follows: "*Natural or legal person providing public communications 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*."	<u>Article 17</u> The Czech Republic is not in line with this Article. <u>Article 30</u> The Czech Republic is not in line with this Article. The T-CY requests the authorities of the Czech Republic to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.

Party	Legal provision and practical experience	Assessment
	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), On the ground of this provision (as far as Article 17 concerns only traffic data) we believe, that we are in line with Article 17 of Budapest Convention.	
5. Denmark	The Administration of Justice Act Section 786a, subsection (3), also provides for the partial disclosure of traffic data: "The Administration of Justice Act Section 786a. (1) In connection with an investigation in which electronic evidence may be of importance, the police may impose orders on providers of telecom networks or services to arrange for emergency protection of electronic data, including traffic data. (2) An order of emergency protection under subsection (1) above may solely comprise electronic data stored at the point in time when the order is imposed. The order must state the data that must be secured and the period for which they must be secured (the period of protection). The order must be limited to comprise solely the data estimated to be necessary for investigation and the protection period must be as short as possible and no more than 90 days. An order of this nature may not be extended. (3) Providers of telecom networks or services are responsible for ensuring as part of the protection under subsection (1) without undue delay that they pass on traffic data concerning other telecom network or service providers whose networks or services have been used in connection with the electronic communication that may be of importance for the investigation. (4) Violation of subsections (1) and (3) above is punishable by a fine." The power seems to be rarely used in domestic proceedings, but is used for international requests.	Article 17 Denmark is in line with this article. Article 30 Denmark is in line with this article.

Party	Legal provision and practical experience	Assessment
6. Dominican Republic	Article 54 of Law 53-07 may be used: Artículo 54.- Facultades del Ministerio Público. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de: b) Ordenar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos; Article 54 of Law 53-07 allows the preservation of data but not the expedited disclosure of traffic data. There is not an express legal possibility to disclose data. Besides, according to the jurisprudence of the Constitutional Court, disclosure of data (all types of data), requires an order from a judge. This requirement can be an obstacle to expedite the disclosure of traffic data. There is no information regarding the practical implementation of these provisions. A ruling of the Constitutional Court TC-200/13 declared the implementing regulation for data retention, preservation and disclosure, unconstitutional; they can therefore not be applied at present. The authorities of the Dominican Republic are currently working on a draft bill to amend law 53/07 to include new elements and take account of the court ruling by preparing new implementing regulations.	Article 17 The Dominican Republic is not in line with this Article. Article 30 The Dominican Republic is not in line with this Article. The T-CY requests the authorities of the Dominican Republic to complete the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.
7. Iceland	In paragraph 47 in the Communications Act 81/2003 it is stated (in Icelandic): *Ekki má án undangengins dómsúrskurðar heimila óviðkomandi aðilum að sjá skeyti,*	Article 17

Party	Legal provision and practical experience	Assessment
	önnur skjöl eða annála um sendingar sem um fjarskiptavirkin fara eða hlusta á fjarskiptasamtöl eða hljóðrita þau. Fjarskiptafyrirtæki er þó rétt og skylt að veita lögreglu, í þágu rannsóknar sakamáls, upplýsingar um hver sé skráður eigandi ákveðins símanúmers og/eða eigandi eða notandi vistfangs (IP-tölu). Um aðgang lögreglu að upplýsingum um fjarskipti skal að öðru leyti fara samkvæmt lögum um meðferð sakamála. This paragraph states that a court order is required to access communication data, but gives an exception that requires service providers to provide the police, as a part of a criminal investigation, sufficient communication data to enable to police to identify the registered owner or user of a telephone number or an IP address. Concerning access of the police to communication data there is also a reference to a more generic law on criminal proceedings. Partial disclosure has not yet been used in practice.	Iceland is in line with this article. <u>Article 30</u> Iceland is in line with this article.
8. Japan	As for preservation, Art. 218 and Art. 197(3) of the Code of Criminal Procedure are used. Traffic data is basically seized. Procedure: (1) Investigating authorities specify the computer data necessary for investigation and the holder(s) of such data. (2) Public prosecutor, public prosecutor's assistant officer or a judicial police official (hereinafter referred to as "investigating officials") drafts the preservation request document and sends it to the data holder [for traffic data only]. (3) Investigating officials request for issuance of a seizure warrant to a judge and receive the warrant. (4) Investigating officials show the seizure warrant to the data holder (service provider) and seize the data specified in the warrant upon submission by the holder.	<u>Article 17</u> Japan is partially in line with this Article. The procedures does not seem sufficiently expeditious and predictable. <u>Article 30</u> Japan is partially in line with this Article. Although data may be disclosed without an MLA request, domestic seizure powers need to be used which does not always seem to allow for expeditious disclosure. The T-CY requests the authorities of Japan to undertake the necessary reforms to bring

Party	Legal provision and practical experience	Assessment
	According to clarification provided by Japan, although seizure powers need to be used to obtain the disclosure of a sufficient amount of traffic data to determine the path of a communication "the authorities presume that it mostly takes 2 weeks to seize traffic data from the moment of preservation of such data, which Japan considers as sufficiently expeditious." With regard to international requests, information provided by Japan states: "It is possible for Japan to expeditiously submit the information which "a service provider in another State was involved in the transmission of the communication" cited in the Article 30, not only through the MLA (Japan expeditiously executes the search, the seizure and the entire disclosure on the basis of MLA) but also through the ICPO channel and the point of contact designated on the basis of the Convention, and Japan thus considers that it is fully in line with Article 30." Comment by Japan: Japan's reply concerning the time frame of two weeks: In Japan, seizure warrants are usually issued in 1 day, and "Two weeks" is a time period ISPs generally take for the preparation for the response to the request. "Two weeks" is simply an average time period and some ISPs are able to respond to the request in a few days. (It is also applied to Article 30.)	domestic regulations and practices in line with the Budapest Convention on Cybercrime.
9. Malta	No information	The T-CY regrets that no information has been received and recalls that under the Rules of Procedure, "T-CY members shall participate in the assessment of the implementation of the Convention".
10. Mauritius	The relevant provisions of the law are sections 12 and 13 of the Computer Misuse and Cybercrime Act 2003: *12. Disclosure of preserved data*	<u>Article 17</u> Mauritius is in line with this Article.

Party	Legal provision and practical experience	Assessment
	The investigatory authority may, for the purposes of a criminal investigation or the prosecution of an offence, apply to the Judge in Chambers for an order for the disclosure of— *(a) all preserved data, irrespective of whether one or more service providers were involved in the transmission of such data;* *(b) sufficient data to identify the service providers and the path through which the data was transmitted; or* *(c) electronic key enabling access to or the interpretation of data*. *13. Production order* *(1) Where the disclosure of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigatory authority may apply to the Judge in Chambers for an order compelling—* *(a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and* *(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.* *(2) Where any material to which an investigation relates consists of data stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.* These provisions are used all the time at the domestic level.	Article 30 Mauritius is not in line with this Article as an MLA request is required. The T-CY requests the authorities of Mauritius to undertake the necessary reforms to bring domestic regulations and practices in line with the Budapest Convention on Cybercrime.
11. Panama	No information	The T-CY regrets that no information has been received and recalls that under the Rules of Procedure, "T-CY members shall participate in the assessment of the implementation of the Convention".

5 Conclusions

Further to the assessment carried out in 2012,[5] the T-CY at its 13th Plenary Session (15-16 June 2015) discussed and adopted the present report assessing the implementation by additional Parties of four articles of the Budapest Convention on Cybercrime:

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

5.1 Conclusions and recommendations

The T-CY,

- 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 and the cooperation in the assessment by nine States;
- regrets that no replies have been received from Malta and Panama;
- calls on all Parties to actively participate in future assessments in the interest of the effectiveness of the Budapest Convention and of efficient international cooperation against cybercrime.

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

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

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

3. 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.

4. 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.

5.2 Summary of implementation by Parties

Party (Y = in line P = Partially in line N = Not in line with the Budapest Convention)	**Article 16 Expedited preservation**	**Article 29 Expedited preservation (international)**	**Article 17 Preservation and partial disclosure**	**Article 30 Preservation and partial disclosure (international)**
1. Australia	P	P	Y	Y
2. Austria	N	N	N	N
3. Belgium	N	N	N	N
4. Czech Republic	P	N	N	N
5. Denmark	Y	P	Y	Y
6. Dominican Republic	Y	Y	N	N
7. Iceland	P	P	Y	Y
8. Japan	Y	Y	P	P
9. Malta	No information	No information	No information	No information
10. Mauritius	Y	N	Y	N
11. Panama	No information	No information	No information	No information

5.3 Follow up

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

The T-CY will review progress made within 18 months of adoption of the report (that is, by end-2016).

6 Appendix: Replies to questionnaire

6.1 Australia

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

Legislation/regulations

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

Divisions 1 and 2 of Part 3-1A of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) establish a legal regime that allows Australian enforcement agencies and the Australian Security Intelligence Organisation (the Organisation) to require carriers (and carriage service providers) to preserve the content of 'stored communications', as well as traffic data associated with those stored communications. These provisions are set out below.

The term 'stored communication' is defined in section 5 of the TIA Act:

> ***stored communication*** means a communication that:
> (a) is not passing over a telecommunications system; and
> (b) is held on equipment that is operated by, and is in the possession of, a carrier; and
> (c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier

The definition of 'stored communication' includes communications such as emails, SMS messages and voicemail messages that are held by carriers or carriage service providers. It does not include those communications when they are stored on an end-user's device, such as emails that have been downloaded to a desktop PC or smartphone.

Subparagraph 107H(1)(b)(ii) creates a class of preservation notice known as an 'ongoing domestic preservation notice'. This class of preservation notice requires a carrier or carriage service provider to preserve stored communications that it holds at the time it receives the notice, as well as any stored communications that it comes to hold in the following 30 days. This class of preservation notice ensures that communications that come into existence after the preservation notice is issued, but before the agency can obtain a warrant, are not lost. This class of preservation notice may be regarded as having a greater impact on privacy. As such, only the Organisation and a limited number of 'interception agencies' may issue such notices. The term 'interception agency' is defined in section 5 of the TIA Act, and includes:

- the Australian Federal Police
- the Australian Commission for Law Enforcement Integrity
- the Australian Crime Commission
- a police force of a State or Territory
- State and Territory Crime Commissions, and
- certain State and Territory anti-corruption and integrity bodies.

Part 3-1A—Preserving stored communications

Division 1—Outline of this Part

107G Outline of this Part

This Part establishes a system of preserving certain stored communications that are held by a carrier. The purpose of the preservation is to prevent the communications from being destroyed before they can be accessed under certain warrants issued under this Act.

Under the system, certain agencies can give a preservation notice to a carrier requiring the carrier to preserve all stored communications that the carrier holds that relate to the person or telecommunications service specified in the notice. The carrier will breach its obligations under section 313 of the *Telecommunications Act 1997* if it does not comply with the notice.

There are 2 types of preservation notices: domestic preservation notices (which cover stored communications that might relate either to a contravention of certain Australian laws or to security) and foreign preservation notices (which cover stored communications that might relate to a contravention of certain foreign laws).

Division 2 deals with domestic preservation notices. There are 2 kinds of domestic preservation notices:

(a) historic domestic preservation notices, which cover stored communications held by the carrier on a particular day; and
(b) ongoing domestic preservation notices, which cover stored communications held by the carrier in a particular 30-day period.

An issuing agency (which is an enforcement agency or the Organisation for an historic domestic preservation notice, and an interception agency or the Organisation for an ongoing domestic preservation notice) can only give a domestic preservation notice if the conditions in section 107J are satisfied. There are certain grounds on which the notice must be revoked (see section 107L).

Division 3 deals with foreign preservation notices. Foreign preservation notices, like historic domestic preservation notices, cover stored communications held by the carrier on a particular day. Only the Australian Federal Police can give a foreign preservation notice to a carrier and it can only do so if a foreign country has made a request for the preservation in accordance with section 107P. There are certain grounds on which the notice must be revoked (see section 107R).

Division 4 has miscellaneous provisions relating to both domestic and foreign preservation notices (such as provisions about the giving of evidentiary certificates by carriers and issuing agencies).

The Ombudsman has functions in relation to preservation notices given by issuing agencies (other than the Organisation) and the Inspector-General of Intelligence and Security has functions in relation to preservation notices given by the Organisation.

Division 2—Domestic preservation notices

107H Domestic preservation notices

(1) An issuing agency may give a carrier a written notice (a domestic preservation notice) requiring the carrier to preserve, while the notice is in force, all stored communications that:
  (a) relate to the person or telecommunications service specified in the notice; and
  (b) the carrier holds at any time during:
    (i) the period that starts at the time the carrier receives the notice and ends at the end of the day the carrier receives the notice (in which case the notice is an historic domestic preservation notice); or
    (ii) the period that starts at the time the carrier receives the notice and ends at the end of the 29th day after the day the carrier receives the notice (in which case the notice is an ongoing domestic preservation notice).

(2) However, the agency can only give the notice if the conditions in subsection 107J(1) or (2) are satisfied.

(3) In the notice, the agency can only specify:
  (a) one person; or
  (b) one or more telecommunications services; or
  (c) one person and one or more telecommunications services.

107J Conditions for giving domestic preservation notices

Notices given by enforcement agencies or interception agencies

(1) A domestic preservation notice may be given under subsection 107H(1) if:
  (a) the issuing agency is:
    (i) for an historic domestic preservation notice—an enforcement agency; and
    (ii) for an ongoing domestic preservation notice—an enforcement agency that is an interception agency; and
  (b) the agency is investigating a serious contravention; and
  (c) the agency considers that there are reasonable grounds for suspecting that, in the relevant period for the notice, there are stored communications in existence, or stored communications might come into existence, that:
    (i) might assist in connection with the investigation; and
    (ii) relate to the person or telecommunications service specified in the notice; and
  (d) the agency intends that if, at a later time, the agency considers that the stored communications would be likely to assist in connection with the investigation, then the agency will apply for a Part 2-5 warrant or a stored communications warrant to access those communications; and
  (e) for an ongoing domestic preservation notice—there is not another ongoing domestic preservation notice in force that:
    (i) was given by the agency to the same carrier; and
    (ii) specifies the same person or telecommunications service.

Notices given by the Organisation

(2) A domestic preservation notice may be given under subsection 107H(1) if:
  (a) the issuing agency is the Organisation; and
  (b) the Organisation considers that there are reasonable grounds for suspecting that, in the relevant period for the notice, there are stored communications in existence, or stored communications might come into existence, that:
    (i) might assist the Organisation in carrying out its function of obtaining intelligence

relating to security; and

(ii) relate to the person or telecommunications service specified in the notice; and

(c) the Organisation intends that if, at a later time, the Organisation considers that the stored communications would be likely to assist in carrying out that function, then the Director-General of Security will request a Part 2-2 warrant to access those communications; and

(d) for an ongoing domestic preservation notice—there is not another ongoing domestic preservation notice in force that:

(i) was given by the Organisation to the same carrier; and

(ii) specifies the same person or telecommunications service.

107K When a domestic preservation notice is in force

A domestic preservation notice:

(a) comes into force when the carrier receives it; and

(b) ceases to be in force at the earliest of the following times:

(i) the end of the period of 90 days, starting on the day the carrier receives it;

(ii) if the notice is revoked under section 107L—when the carrier receives notice of the revocation;

(iii) if a Part 2-5 warrant or stored communications warrant authorising access to the stored communications covered by the notice is issued in relation to the issuing agency—when the warrant ceases to be in force;

(iv) if a Part 2-2 warrant authorising access to the stored communications covered by the notice is issued in relation to the issuing agency—the end of the period of 5 days after the day the warrant was issued.

107L Revoking a domestic preservation notice

Discretionary revocation

(1) An issuing agency that has given a domestic preservation notice may revoke the notice at any time.

Mandatory revocation

(2) An issuing agency that has given a domestic preservation notice must revoke the notice if:

(a) if the issuing agency is an enforcement agency (including an interception agency):

(i) the condition in paragraph 107J(1)(b) or (c) is no longer satisfied; or

(ii) the agency decides not to apply for a Part 2-5 warrant or stored communications warrant to access the stored communications covered by the notice; or

(b) if the issuing agency is the Organisation:

(i) the condition in paragraph 107J(2)(b) is no longer satisfied; or

(ii) the Organisation is satisfied that the Director-General of Security will not request a Part 2-2 warrant to access the stored communications covered by the notice.

Revocation effected by giving revocation notice

(3) A domestic preservation notice is revoked by the issuing agency giving the carrier to whom it was given written notice of the revocation.

107M Persons who act on the issuing agency's behalf

Historic domestic preservation notices

(1) An historic domestic preservation notice may only be given or revoked on behalf of an issuing agency by:
  (a) if the issuing agency is an enforcement agency—a person who may, under section 110, apply on the agency's behalf for a stored communications warrant to access the stored communications covered by the notice; and
  (b) if the issuing agency is the Organisation—a certifying person.

Ongoing domestic preservation notices

(2) An ongoing domestic preservation notice may only be given on behalf of an issuing agency by:
  (a) if the issuing agency is an enforcement agency that is an interception agency—an authorised officer of the agency; and
  (b) if the issuing agency is the Organisation—the Director-General of Security.

(3) An ongoing domestic preservation notice may only be revoked on behalf of an issuing agency by:
  (a) if the issuing agency is an enforcement agency that is an interception agency—an authorised officer of the agency; and
  (b) if the issuing agency is the Organisation—a certifying person.

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

As outlined in our response to Q 1.1.1, Australian preservation notices only cover content and traffic data that is associated with 'stored communications'. Australian preservation notices are not available for traffic data associated with other types of communications.

The reason why Australian preservation notices do not cover other types of traffic data is that the legal regime for *access* to traffic data allows enforcement agencies to access traffic data in a timely fashion when it is required for an investigation. As such, the Australian Government considers that it is unnecessary to implement a separate preservation notice regime for traffic data.

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

Section 107J of the TIA Act provides that Australian enforcement agencies may only issue a preservation notice where:

(1) The agency is investigating a 'serious contravention', which is defined as:
  (a) an offence punishable by at least 3 years' imprisonment; or
  (b) in the case of an offence or contravention committed by an individual, an offence or contravention punishable by a fine or pecuniary penalty of at least 180 penalty units (A$30,600); or
  (c) in the case of an offence or contravention that cannot be committed by an individual, an offence or contravention punishable by a fine or pecuniary penalty of at least 900 penalty units (A$153,000); and

(2) The agency intends that if, at a later time, the agency considers that the stored content would be likely to assist with the investigation, then the agency will apply for a warrant to access those communications.

This limitation is consistent with the limitation on the offences for which Australian enforcement agencies may apply for a warrant to access stored content, including stored content that has been preserved.

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

The *Privacy Act 1988* permits (but does not require) private sector holders of personal information to preserve personal information where they 'reasonably believe that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.' This permission is an exception from the general obligation to destroy or de-identify personal information that is no longer needed for any purpose for which it may be lawfully used or disclosed, and that is not required by law or a court or tribunal order to be kept. Under the *Privacy Act 1988*, enforcement bodies may only request information—they cannot use the *Privacy Act 1988* to compel private sector companies to preserve data.

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

In Australia, preservation is not generally visible to the suspects or account-holder. Section 133 of the TIA Act prohibits communicating 'preservation notice information' to another person without lawful authority. Preservation notice information includes information about the existence or non-existence of a preservation notice, or any other information that is likely to enable the identification of the person or telecommunications service specified in a preservation notice or to which a notice relates.

Procedures

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

Preservation
Step 1 — Request by agency to carrier (section 107H, TIA Act)
Step 2 — End of preservation notice (sections 107K and 107L, TIA Act)

Access
Step 1 — Application to issuing officer (section 110, TIA Act)
Step 2 — Consideration of application for warrant (section 116, TIA Act)
Step 3 — Use of stored communications warrant (section 117, TIA Act)

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

There is no prescribed template or form for a domestic preservation notice.

Practical experience

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?

This information was not available at the time of completing this questionnaire.

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

This information was not available at the time of completing this questionnaire. We anticipate that this information will be available following the release of the Annual Report for the *Telecommunications (Interception and Access) Act 1979* for 2013-14.

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?

As explained above, Divisions 1 and 2 of Part 3-1A of the TIA Act specifically provide for the preservation of stored content and associated traffic data.

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

The preservation notice regime under Divisions 1 and 2 of Part 3-1A of the TIA Act applies only to carriers and carriage service providers.

As explained in our response to question 1.1.4, Australian enforcement agencies may *request* that other physical or legal persons preserve data, however they do not have the power to compel other physical or legal persons to preserve data.

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

This information was not available at the time of completing this questionnaire.

Please describe a typical case or scenario.

This information was not available at the time of completing this questionnaire.

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

This information was not available at the time of completing this questionnaire.

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

Legislation/regulations

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

As noted in our response to Q 1.1.2, Australian preservation notices only cover content and traffic data that is associated with 'stored communications'. Australian preservation notices are not available for traffic data associated with other types of communications.

The reason why Australian preservation notices do not cover other types of traffic data is that the legal regime for *access* to traffic data allows enforcement agencies to access traffic data in a timely fashion when it is required for an investigation. As such, the Australian Government considers that it is unnecessary to implement a separate preservation notice regime for traffic data.

Divisions 4 and 4B of Part 4-1 of the TIA Act regulate access to traffic data by Australian enforcement agencies. Sections 276, 277 and 278 of the *Telecommunications Act 1997*, which are referred to throughout Division 4, make it a criminal offence for the employees of carriers, carriage service providers, and other entities that hold communications-related information to disclose such information (or a document containing such information), except where it is expressly required or authorised by or under law.

Division 4—Enforcement agencies

177 Voluntary disclosure

Enforcement of the criminal law

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure by a person (the holder) of information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of the criminal law.

Enforcement of a law imposing a pecuniary penalty or protection of the public revenue

(2) Sections 276 and 277 of the *Telecommunications Act 1997* do not prevent a disclosure by a person (the holder) of information or a document to an enforcement agency if the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Limitation

(3) This section does not apply if a relevant staff member of an enforcement agency requests the holder to disclose the information or document.

Note: Sections 178 to 180 deal with the disclosure of information or a document in response to authorisations by an authorised officer of an enforcement agency.

178 Authorisations for access to existing information or documents—enforcement of the criminal law

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).

(2) An authorised officer of an enforcement agency may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

(3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law.

178A Authorisations for access to existing information or documents—locating missing persons

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).

–

(2) An authorised officer of the Australian Federal Police, or a Police Force of a State, may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

(3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the purposes of finding a person who the Australian Federal Police, or a Police Force of a State, has been notified is missing.

179 Authorisations for access to existing information or documents—enforcement of a law imposing a pecuniary penalty or protection of the public revenue

(1) Sections 276 and 277 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).

–

(2) An authorised officer of an enforcement agency may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

(3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue.

Division 4B—Privacy to be considered when making authorisations

180F Authorised officers to consider privacy

Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to the following matters:

(a) the likely relevance and usefulness of the information or documents;

(b) the reason why the disclosure or use concerned is proposed to be authorised.

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

As noted in response to question 2.1.1, sections 276, 277 and 278 of the *Telecommunications Act 1997* make it a criminal offence for an employee of a carrier, carriage service provider or other entity

that holds communications-related information to disclose such information, except where it is expressly required or authorised by or under law.

Procedures

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

N/A

Practical experience

How relevant to investigations in your country is partial disclosure?

Access to telecommunications data is a critical investigative tool for law enforcement investigations. Electronic communications, by definition, do not leave a physical footprint, allowing individuals and groups to plan and carry out such activities without risk of detection via many 'traditional' investigative techniques. As such, the records kept by telecommunications companies about the services they have provided (telecommunications data) are often the only source of information available to agencies to identify and investigate individuals and groups using communications technologies for such purposes.

Telecommunications data is accessed and used by Australian enforcement agencies to:

- identify suspects and/or victims
- remove innocent and uninvolved persons from suspicion, and from further, more intrusive investigation
- resolve life threatening situations like child abduction or exploitation
- identify associations between members of criminal organisations
- provide insight into criminal syndicates and terrorist networks, and
- establish leads to target further investigative resources.

Between July and September 2014, telecommunications data was used in 92 per cent of counterterrorism investigations, 100 per cent of cybercrime investigations, 87 per cent of child protection investigations and 79 per cent of serious organised crime investigations conducted by the Australian Federal Police.

In February 2015, Australia's Parliamentary Joint Committee on Intelligence and Security released a major report which concluded *inter alia* that:

> The value of telecommunications data to national security and law enforcement investigations is indisputable. Its value is rising as criminals and persons engaged in activities prejudicial to security increasingly rely on communications technology to plan, facilitate and carry out their activities, while the ability of agencies to lawfully intercept the content of those communications declines.[6]

How frequently do you use these provisions?

[6] Parliamentary Joint Committee on Intelligence and Security, Parliament of Australia, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (2015) 69. Available online at <http://www.aph.gov.au/~/media/02%20Parliamentary%20Business/24%20Committees/244%20Joint%20Committees/PJCIS/DataRetention2014/FinalReport_27February2015.pdf>

Australian enforcement agencies made a total of 319,874 authorisations for access to historic telecommunications data in 2012-13.

This figure includes authorisations that relate solely to subscriber or account-holder records, as well as authorisations for the disclosure of traffic data. Separate figures are not available for these two categories of telecommunications data. Additionally, Australian law requires agencies to make a separate authorisation (involving a separate consideration of the necessity and interference with privacy of access to the specific telecommunications data requested) on each occasion that an agency seeks access to telecommunications data; Australian law does not permit agencies to make a single authorisation for the disclosure of telecommunications data in connection with a given investigation.

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

This information was not available at the time of completing this questionnaire.

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

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

Legislation/regulations

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

Under section 107P of the *Telecommunications (Interception and Access) Act 1979* (TIA Act), a foreign country can make a request to the Australian Federal Police (AFP) to arrange for the preservation of certain stored communications if that country intends to make a formal mutual assistance request to access those communications. Upon receiving a request from a foreign country, the AFP must give the carrier a written notice requiring the carrier to preserve all stored communications relevant to the person or telecommunications service in question that is held by the carrier at any time between when it receives the request and the end of that day.

107P Condition for giving a foreign preservation notice

(1) If, under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987*, a foreign country intends to request the Attorney-General to arrange for access to stored communications that:

(a) relate to a specified person or specified telecommunications service; and

(b) are held by a carrier; and

(c) are relevant to an investigation, or investigative proceeding, relating to a criminal matter involving a serious foreign contravention;

then the foreign country may request the Australian Federal Police to arrange for the preservation of those stored communications.

(2) The request to the Australian Federal Police must:

(a) be in writing; and

(b) specify the name of the authority concerned with the criminal matter; and

(c) specify the serious foreign contravention that is the subject of the investigation or investigative proceeding; and

(d) specify information identifying the stored communications to be preserved and the relationship between those communications and the serious foreign contravention; and

(e) specify any information the foreign country has that identifies the carrier that holds the stored communications; and

(f) if the stored communications relate to a specified person—specify any information the foreign country has that identifies the telecommunications service to which the stored communications relate; and

(g) specify the reasons why the stored communications need to be preserved; and

(h) specify that the foreign country intends to make a request under paragraph 15B(d) of the *Mutual Assistance in Criminal Matters Act 1987* to access the stored communications.

107N When a foreign preservation notice can be given

(1) If the Australian Federal Police receives a request in accordance with section 107P, the Australian Federal Police must give the carrier to which the request relates a written notice (a ***foreign preservation notice***) requiring the carrier to preserve, while the notice is in force, all stored communications that:

(a) relate to the person or telecommunications service specified in the notice; and

(b) the carrier holds at any time during the period that starts at the time the carrier receives the notice and ends at the end of the day the carrier receives the notice.

(2) In the notice, the Australian Federal Police can only specify:

(a) one person; or

(b) one or more telecommunications services; or

(c) one person and one or more telecommunications services.

107Q When a foreign preservation notice is in force

A foreign preservation notice:

(a) comes into force when the carrier receives it; and

(b) ceases to be in force at the earlier of the following times:

(i) if the notice is revoked under section 107R—when the carrier receives notice of the revocation;

(ii) if a stored communications warrant authorising access to the stored communications covered by the notice is issued after the Attorney-General has given an authorisation in relation to the warrant under section 15B of the *Mutual Assistance in Criminal Matters Act 1987*—when the warrant ceases to be in force.

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

AOCC Watchfloor Operations
Australian Federal police
GPO Box 401
Canberra ACT 2601
Australia

E-Mail: AOCC-Watchfloor-Supervisor@afp.gov.au
Tel: + 61 2 6126 7299
Fax: + 61 2 6126 7910

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

There are certain rules applying to the preservation and transfer of preserved data set out in the text and provisions below.

Preservation

In addition to the requirements at paragraph 107P(1)(a) and 107P(b), paragraph 107P(1)(c) of the TIA Act requires the communications to be relevant to an investigation, or investigative proceeding, relating to a criminal matter involving a 'serious foreign contravention'. Section 5EA of the TIA Act defines 'serious foreign contravention' as a contravention of a law of a foreign country that is punishable by a maximum penalty of:

(b) imprisonment for 3 years or more, imprisonment for life or the death
- penalty; or

(b) a fine of an amount that is at least equivalent to 900 penalty units (that is, A$153,000).

Access

If a country makes a formal request to access communications for foreign law enforcement purposes, the Australian Attorney-General may, in his or her discretion, authorise the AFP or a police force of a State or Territory under section 15B of the *Mutual Assistance in Criminal Matters Act 1987* (MA Act) to apply for a stored communications warrant if satisfied of certain criteria (see below). Once so authorised, a police officer can apply to an 'issuing authority' (judge, magistrate or nominated Administrative Appeals Tribunal member) for a warrant under the TIA Act (section 110, TIA Act). The issuing authority may, under section 116 of the TIA Act, issue a warrant if satisfied of certain criteria (see below). A stored communications warrant authorises the person to access, subject to any conditions or restrictions that are specified in the warrant, the stored communications (section 117, TIA Act). The material can then be provided to the foreign country subject to sections 139, 142 and 142A of the TIA Act.

Mutual Assistance in Criminal Matters Act 1987

15B Requests by foreign countries for stored communications

The Attorney-General may, in his or her discretion, authorise the Australian Federal Police or a police force or police service of a State, in writing, to apply for a stored communications warrant under section 110 of the *Telecommunications (Interception and Access) Act 1979* if the Attorney-General is satisfied that:

(a) an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of a foreign country (the ***requesting country***) has commenced in the requesting country; and

(b) the offence to which the investigation, or investigative proceeding, relates is punishable by a maximum penalty of:
  (i) imprisonment for 3 years or more, imprisonment for life or the death penalty; or
  (ii) a fine of an amount that is at least equivalent to 900 penalty units; and

(c) there are reasonable grounds to believe that stored communications relevant to the investigation, or investigative proceeding, are held by a carrier; and

(d) the requesting country has requested the Attorney-General to arrange for access to the stored communications.

Note: Information obtained under the warrant may only be communicated to the requesting country on certain conditions: see subsection 142A(1) of the *Telecommunications (Interception and Access) Act 1979*.

Telecommunications (Interception and Access) Act 1979

110 Enforcement agencies may apply for stored communications warrants

(1) An enforcement agency may apply to an issuing authority for a stored communications warrant in respect of a person.

(2) The application must be made on the agency's behalf by:
(a) if the agency is referred to in subsection 39(2)—a person referred to in that subsection in relation to that agency; or
(b) otherwise:
(i) the chief officer of the agency; or
(ii) an officer of the agency (by whatever name called) who holds, or is acting in, an office or position in the agency nominated under subsection (3).

(3) The chief officer of the agency may, in writing, nominate for the purposes of subparagraph (2)(b)(ii) an office or position in the agency that is involved in the management of the agency.

(4) A nomination under subsection (3) is not a legislative instrument.

116 Issuing of stored communications warrants

(1) An issuing authority to whom an enforcement agency has applied for a stored communications warrant in respect of a person may, in his or her discretion, issue such a warrant if satisfied, on the basis of the information given to him or her under this Part in connection with the application, that:
(a) Division 1 has been complied with in relation to the application; and
(b) in the case of a telephone application—because of urgent circumstances, it was necessary to make the application by telephone; and
(c) there are reasonable grounds for suspecting that a particular carrier holds stored communications:
(i) that the person has made; or
(ii) that another person has made and for which the person is the intended recipient; and
(d) information that would be likely to be obtained by accessing those stored communications under a stored communications warrant would be likely to assist in connection with:
(i) in the case of an application other than a mutual assistance application—the investigation by the agency of a serious contravention in which the person is involved (including as a victim of the serious contravention); or
(ii) in the case of a mutual assistance application—the investigation or investigative proceeding, by the foreign country to which the application relates, of a serious foreign contravention to which the application relates and in which the person is involved (including as a victim of the serious foreign contravention); and
(da) if the stored communications warrant is applied for in relation to a person who is the victim of the serious contravention—the person is unable to consent, or it is impracticable for the person to consent, to those stored communications being accessed; and

(e) in any case—having regard to the matters referred to in subsection (2) or (2A) (as the case requires), and to no other matters, the issuing authority should issue a warrant authorising access to such stored communications.

(2) In the case of an application other than a mutual assistance application, the matters to which the issuing authority must have regard are:

(a) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and

(b) the gravity of the conduct constituting the serious contravention; and

(c) how much the information referred to in subparagraph (1)(d)(i) would be likely to assist in connection with the investigation; and

(d) to what extent methods of investigating the serious contravention that do not involve the use of a stored communications warrant in relation to the person have been used by, or are available to, the agency; and

(e) how much the use of such methods would be likely to assist in connection with the investigation by the agency of the serious contravention; and

(f) how much the use of such methods would be likely to prejudice the investigation by the agency of the serious contravention, whether because of delay or for any other reason.

(2A) In the case of a mutual assistance application, the matters to which the issuing authority must have regard are:

(a) how much the privacy of any person or persons would be likely to be interfered with by accessing those stored communications under a stored communications warrant; and

(b) the gravity of the conduct constituting the serious foreign contravention; and

(c) how much the information referred to in subparagraph (1)(d)(ii) would be likely to assist in connection with the investigation, to the extent that this is possible to determine from information obtained from the foreign country to which the application relates.

(3) The warrant may be issued in relation to the investigation of more than one serious contravention or serious foreign contravention, but cannot relate to both a serious contravention and a serious foreign contravention.

117 What stored communications warrants authorise

A stored communications warrant authorises persons approved under subsection 127(2) in respect of the warrant to access, subject to any conditions or restrictions that are specified in the warrant, a stored communication:

(a) that was made by the person in respect of whom the warrant was issued; or

(b) that another person has made and for which the intended recipient is the person in respect of whom the warrant was issued;

and that becomes, or became, a stored communication before the warrant is first executed in relation to the carrier that holds the communication.

139 Dealing for purposes of investigation etc.

(1) An officer or staff member of an enforcement agency or an eligible Commonwealth authority may, for one or more purposes referred to in subsection (2) or (4A), and for no other purpose (other than a purpose referred to in subsection 139A(2), if applicable), communicate to another person, make use of, or make a record of the following:

(a) lawfully accessed information other than foreign intelligence information;

(aa) preservation notice information;

(b) stored communications warrant information.

(2) In the case of information obtained by the agency other than through the execution of a warrant issued as a result of a mutual assistance application, the purposes are purposes connected with:

(a) an investigation by the agency or by another enforcement agency of a contravention to which subsection (3) applies; or

(b) the making by an authority, body or person of a decision whether or not to begin a proceeding to which subsection (4) applies; or

(c) a proceeding to which subsection (4) applies; or

(d) the keeping of records by the agency under Part 3-5; or

(e) an authorisation under subsection 13A(1) of the *Mutual Assistance in Criminal Matters Act 1987* in respect of the information.

(3) A contravention to which this subsection applies is a contravention of a law of the Commonwealth, a State or a Territory that:

(a) is a serious offence; or

(b) is an offence punishable:

(i) by imprisonment for a period, or a maximum period, of at least 12 months; or

(ii) if the offence is committed by an individual—by a fine, or a maximum fine, of at least 60 penalty units; or

(iii) if the offence cannot be committed by an individual—by a fine, or a maximum fine, of at least 300 penalty units; or

(c) could, if established, render the person committing the contravention liable:

(i) if the contravention were committed by an individual—to pay a pecuniary penalty of 60 penalty units or more, or to pay an amount that is the monetary equivalent of 60 penalty units or more; or

(ii) if the contravention cannot be committed by an individual—to pay a pecuniary penalty of 300 penalty units or more, or to pay an amount that is the monetary equivalent of 300 penalty units or more.

(4) A proceeding to which this subsection applies is:

(a) a proceeding by way of a prosecution for an offence of a kind referred to in paragraph (3)(a) or (b); or

(b) a proceeding for the confiscation or forfeiture of property, or for the imposition of a pecuniary penalty, in connection with the commission of such an offence; or

(ba) a proceeding under the *Spam Act 2003*; or

(c) a proceeding for the taking of evidence pursuant to section 43 of the *Extradition Act 1988*, in so far as the proceeding relates to such an offence; or

(d) a proceeding for the extradition of a person from a State or a Territory to another State or Territory, in so far as the proceeding relates to such an offence; or

(e) a proceeding for recovery of a pecuniary penalty for a contravention of a kind referred to in paragraph (3)(c); or

(f) a police disciplinary proceeding.

(4A) In the case of information obtained by the agency through the execution of a warrant issued as a result of a mutual assistance application, the purposes are purposes connected with:

(a) providing the information to the foreign country, or an appropriate authority of the foreign country, to which the application relates; or

(b) the keeping of records by the agency under Part 3-5.

(5) To avoid doubt, a reference in subsection (3) to a number of penalty units in relation to a contravention of a law of a State or a Territory includes a reference to an amount of a fine or pecuniary penalty that is equivalent, under section 4AA of the *Crimes Act 1914*, to that number of penalty units.

142 Further dealing by recipient of certain information

A person to whom information has, in accordance with subsection 135(4), section 139 or 139A, subsection 140(2) or this section, been communicated for a purpose, or for 2 or more purposes, may:

(a) communicate that information to another person; or

(b) make use of, or make a record of, that information;

for that purpose, or for one or more of those purposes, and for no other purpose.

142A Communicating information obtained as a result of a mutual assistance application to foreign country

(1) Despite subsection 139(4A) and section 142, a person may only communicate information, obtained through the execution of a warrant issued as a result of a mutual assistance application, to the foreign country to which the application relates, subject to the following conditions:
   (a) that the information will only be used for the purposes for which the foreign country requested the information;
   (b) that any document or other thing containing the information will be destroyed when it is no longer required for those purposes;
   (c) any other condition determined, in writing, by the Attorney-General.

(2) A determination made under paragraph (1)(c) is not a legislative instrument.

Procedures

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

Preservation
Step 1 — Request by foreign country to AFP (section 107P, TIA Act)
Step 2 — Request by AFP to carrier (section 107N, TIA Act)
Step 3 — End of preservation notice (sections 107Q and 107R, TIA Act)

Access
Step 1 — Request by foreign country
Step 2 — Attorney-General authorisation (section 15B, MA Act)
Step 3 — Application to issuing officer (section 110, TIA Act)
Step 4 — Consideration of application for warrant (section 116, TIA Act)
Step 5 — Use of stored communications warrant (section 117, TIA Act)
Step 6 — Provision of material to foreign country (sections 139, 142 and 142A, TIA Act)

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

There is no prescribed template or form for an international request for preservation. Requests must be in writing, and must contain the information specified in section 107P of the TIA Act.

Access
Foreign mutual assistance requests may come in a number of forms. Section 11 of the MA Act requires incoming requests for assistance to include or be accompanied by the following information:

(a) the name of the authority concerned with the criminal matter to which the request relates;
(b) a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;
(c) a description of the purpose of the request and of the nature of the assistance being sought;
(d) any information that may assist in giving effect to the request.

However, a failure to comply with this provision is not a ground for refusing the request.

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

Preservation

The request would need to include information that the relevant offence was a 'serious foreign contravention'. This is because, in addition to the requirements at paragraph 107P(1)(a) and 107P(b), paragraph 107P(1)(c) of the TIA Act requires the communications to be relevant to an investigation, or investigative proceeding, relating to a criminal matter involving a 'serious foreign contravention'. Section 5EA of the TIA Act defines 'serious foreign contravention' as a contravention of a law of a foreign country that is punishable by a maximum penalty of:

1. imprisonment for 3 years or more, imprisonment for life or the death
(1) penalty; or
(b) a fine of an amount that is at least equivalent to 900 penalty units (that is, A$153,000).

Access

Any request must include sufficient information to satisfy the legislative requirements. That is, to meet the criteria thereby allowing the Attorney-General to authorise a police officer to apply for a stored communications warrant (section 15B, MA Act) and satisfy a judge, magistrate or nominated Administrative Appeals Tribunal member of the requirements in relation to issuing a warrant (section 116, TIA Act—e.g. that there are reasonable grounds for suspecting that a particular carrier holds stored communications that the person has made or that another person has made). For example, section 15B of the MA Act requires the Attorney-General to be satisfied that:

(a) an investigation, or investigative proceeding, relating to a criminal matter involving an offence against the law of a foreign country (the ***requesting country***) has commenced in the requesting country; and
(b) the offence to which the investigation, or investigative proceeding, relates is punishable by a maximum penalty of:
    (i) imprisonment for 3 years or more, imprisonment for life or the death penalty; or
    (ii) a fine of an amount that is at least equivalent to 900 penalty units; and
(c) there are reasonable grounds to believe that stored communications relevant to the investigation, or investigative proceeding, are held by a carrier; and
(d) the requesting country has requested the Attorney-General to arrange for access to the stored communications.

Practical experience

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

In 2012-13, the most recent year for which publicly-available figures were available, the Australian Federal Police did not issue any foreign preservation notices.

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

This information was not available at the time of completing this questionnaire.

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

This information was not available at the time of completing this questionnaire.

Please describe a typical case or scenario.

This information was not available at the time of completing this questionnaire.

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

Yes. Provisions on preservation ensure that there is a process in place to seek to preserve records prior to those records being obtained formally. This ensures communications are not destroyed by a carrier or carriage service provider as part of their normal business practices before those communications are able to be lawfully accessed under warrant by a law enforcement agency. Where no such preservation processes are in place, data can be lost, which has an impact on the ability to successfully investigate and prosecute a matter, and may also create difficulties in meeting the criteria under section 15B (c) of the MA Act, namely, that there are reasonable grounds to believe that the stored communications are held by a carrier. Further, resources may be wasted in seeking records via formal mutual assistance request where those records may no longer exist.

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

In 2012-13, the most recent year for which publicly-available figures were available, the Australian Federal Police did not issue any foreign preservation notices.

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

This information was not available at the time of completing this questionnaire.

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

This information was not available at the time of completing this questionnaire.

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

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

Legislation/regulations

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.

Under section 180A of the TIA Act, after receiving a request from a foreign country, an authorised officer of the AFP may authorise a carrier or carriage service provide to disclose to the AFP preserved traffic data where the officer is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country. Following receipt of the preserved traffic data, the officer can authorise the disclosure of the data to a foreign law enforcement agency if satisfied of certain criteria (sections 180A and 180F, TIA Act). A person must not disclose preserved traffic data to a foreign law enforcement agency unless the disclosure is subject to the following conditions:

- that the information will only be used for the purposes for which the foreign country requested it, and
- the information will be destroyed where it is no longer required.

180A Authorisations for access to existing information or documents—enforcement of the criminal law of a foreign country

Disclosure to the Australian Federal Police

(1) Sections 276, 277 and 278 of the *Telecommunications Act 1997* do not prevent a disclosure of information or a document if the information or document is covered by an authorisation in force under subsection (2).

(2) An authorised officer of the Australian Federal Police may authorise the disclosure of specified information or specified documents that came into existence before the time the person from whom the disclosure is sought receives notification of the authorisation.

Note: Section 184 deals with notification of authorisations.

(3) The authorised officer must not make the authorisation unless he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country.

Disclosure to a foreign law enforcement agency

(4) If specified information or specified documents are disclosed because of an authorisation given under subsection (2), an authorised officer of the Australian Federal Police may authorise the disclosure of the information or documents so disclosed to a foreign law enforcement agency.

(5) The authorised officer must not make the authorisation unless he or she is satisfied that:
   (a) the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and
   (b) the disclosure is appropriate in all the circumstances.

180E Disclosing information etc. obtained to foreign country

(1) A person must not disclose information or a document in accordance with an authorisation under section 180A, 180B or 180C to a foreign country unless the disclosure is subject to the following conditions:
   (a) that the information will only be used for the purposes for which the foreign country requested the information;
   (b) that any document or other thing containing the information will be destroyed when it is no longer required for those purposes;
   (c) in the case of information or a document disclosed under section 180B—any other condition determined, in writing, by the Attorney-General.

(2) A determination made under paragraph (1)(c) is not a legislative instrument.

180F Authorised officers to consider privacy

Before making an authorisation under Division 4 or 4A in relation to the disclosure or use of information or documents, the authorised officer considering making the authorisation must have regard to whether any interference with the privacy of any person or persons

that may result from the disclosure or use is justifiable, having regard to the following matters:

(a) the likely relevance and usefulness of the information or documents;

(b) the reason why the disclosure or use concerned is proposed to be authorised.

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

There are certain conditions and limitations applying to the disclosure of traffic data set out in the text and provisions below.

The provision of preserved traffic data would be subject to the conditions and limitations stipulated in the legislation. For example, under subsection 180A(5) of the TIA Act, an authorised officer must not make an authorisation to disclose the data unless satisfied that:

(a) the disclosure is reasonably necessary for the enforcement of the criminal law of a foreign country; and

(b) the disclosure is appropriate in all the circumstances.

Similarly, under subsection 180E(1), a disclosure can only be made where the following conditions are met

(a) the information will only be used for the purposes for which the foreign country requested the information; and

(b) any document or other thing containing the information will be destroyed when it is no longer required for those purposes.

Further, before making such an authorisation, section 180F requires the authorised officer to have regard to whether any interference with the privacy of any person or persons that may result from the disclosure or use is justifiable, having regard to:

(a) the likely relevance and usefulness of the information or documents;

(b) the reason why the disclosure or use concerned is proposed to be authorised.

Procedures

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

Step 1 — Request by foreign country
Step 2 — AFP authorisation to require carrier/carriage service provider to disclose data (section 180A, TIA Act)
Step 3 — Disclosure to a foreign law enforcement agency (sections 180A and 180F, TIA Act)
Step 4 — Conditions attaching to disclosure of information or documents (section 180E, TIA Act).

Practical experience

How frequently do you use this provision?

In 2012/13—the most recent year for which figures are available—the Australian Federal Police made 4 data authorisations for access to historical telecommunications data to enforce the criminal law of a foreign country.

Please describe a typical case or scenario.

This information was not available at the time of completing this questionnaire.

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

Yes. Partial disclosure is a streamlining process that enables law enforcement and prosecutorial agencies to obtain data without having to obtain those records via a formal mutual assistance request. If a country has no processes in place allowing partial disclosure of this information, this affects the timing and resources involved in an investigation and prosecution. This is because firstly, it is a more time-intensive process seeking to make and action a formal government-to-government mutual assistance request (rather than agency-to-agency assistance) and secondly, extra resources are used to make a formal request where there is no guarantee that the relevant records will be held by the relevant carrier.

6.1.5 Additional information provided 11 June 2015 by the Attorney General's Office

Regarding Articles 16 and 29 Budapest Convention:

- Do your provisions indeed only cover service providers and not all holders of data?

  These provisions only cover telecommunications carriers and carriage service providers as defined under the *Telecommunications Act 1997*.

- Do you allow for the preservation of subscriber information?

  No. However, under the Australian scheme preservation of traffic and subscriber data is not necessary as the disclosure authorisation process operates just as quickly as a preservation process. The disclosure of non-content data, including subscriber information, is authorised by law enforcement officials. This is a similarly expeditious process as issuing a preservation notice. By comparison, access to the content of communications is carried out under judicially-approved warrant, which is a slower process that requires the support of a preservation regime. There is no practical necessity for Australian law to incorporate a preservation scheme for non-content data.

- Is preservation available for all offences covered by Articles 2-11 Budapest Convention even if these are not serious crime?

  The following answers are to be read subject to Australia's reservations to the Budapest Convention:

  > *In accordance with Article 42 and Article 22, paragraph 2, of the Convention, Australia reserves the right not to apply the jurisdiction rules laid down in Article 22, paragraph 1.b-d, to offences established in accordance with Article 7 (Computer-related forgery), Article 8 (Computer-related fraud) and Article 9 (Offences related to child pornography). The Parliament of the Commonwealth of Australia does not enjoy a plenary power to make laws establishing offences for computer-related forgery, computer-related fraud or offences related to child pornography. The Parliament of the Commonwealth of Australia has established offences for computer-related forgery, computer-related fraud and offences related to child pornography, committed on board ships flying Australian flags, on board aircraft registered under Australian*

law, or by Australian nationals outside Australia, where the offending conduct involves some subject matter with respect to which it has legislative power. In addition to those offences, the Australian States and Territories have also established offences in accordance with Articles 7, 8 and 9 when committed on their territory.

In accordance with Article 42 and Article 22, paragraph 2, of the Convention, Australia further reserves the right not to apply the jurisdiction rules laid down in Article 22, paragraphs 1.b-d, to offences established in accordance with Article 10 (Offences related to infringements of copyright and related rights). Australian law does not presently provide jurisdiction over acts constituting infringements of copyright and related rights committed on board ships flying Australian flags, on board aircraft registered under Australian law, or by Australian nationals outside Australia.

Expeditious access to telecommunications data is available for the investigation of all criminal offences, including all offences covered by Articles 2-11 of the Budapest Convention. As noted above, because Australian access arrangements for telecommunications data operate just as quickly as preservation notices, Australia does not have preservation notices for telecommunications data.

In relation to the content of stored communications held by carriers and carriage services providers, preservation notices will be available in relation to all offences covered by Articles 2 and 4-10 of the Budapest Convention. Preservation will only be available for a limited range of offences covered by Article 3 of the Budapest Convention (Illegal interception), where the offence relates to a criminal organisation. The unlawful interception of communications is punishable by 2 years' imprisonment in Australia, and so does not constitute a 'serious contravention' that would allow agencies to obtain a preservation notice. The illegal interception of communications will only constitute a serious contravention where the offence involves aiding, abetting, counselling or procuring the illegal interception of communications for a criminal organisation, or being, by act or omission, in any way, directly or indirectly, knowingly concerned in, or party to, the illegal interception of communications for a criminal organisation, or conspiring to illegally intercept communications for a criminal organisation.

Preservation notices will be available for all offences covered by Article 11, except for offences involving aiding, abetting or attempting the commission of offences covered by Article 3 (Illegal interception) that are not 'serious contraventions' under Australian law.

Regarding Articles 17 and 30:

- Which provisions would allow for the expedited disclosure of a sufficient amount of traffic data to determine the path of a communication?

  Sections 178-179 of the *Telecommunications (Interception and Access) Act 1979* (TIA Act) allows for the expedited disclosure of a sufficient amount of traffic data to determine the path of a communication to Australian law enforcement agencies. Section 180A of the TIA Act allows for similarly expedited disclosures of traffic data to the Australian Federal Police for foreign law enforcement purposes.

- Could you disclose such data to foreign authorities without an MLA?

Yes. Under section 180A of the TIA Act, the Australian Federal Police is able to authorise the disclosure of non-content data (traffic and subscriber) for the purposes of foreign law enforcement, and to disclose that information to foreign LEAs without an MLA request. Section 180C of the TIA Act also allows the Australian Federal Police to disclose non-content data that has been obtained using domestic powers (except for under section 178A, which relates to non-criminal missing person investigations) to foreign LEAs without an MLA request.

The ability to disclose non-content data to foreign LEAs is subject to the conditions set out in sections 180E and 180F. In particular, section 180E requires that:

(a) the information must only be used for the purposes for which the foreign country requested the information;
(b) that any document or other thing containing the information must be destroyed when it is no longer required for those purposes.

- If so, would this be available for all offences under Articles 2-11 or only to serious crime?

The expedited disclosure of traffic data is available for all offences under Articles 2-11.

6.2 Austria

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

1.1.Legislation/regulations

Q1.1.1 What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

1. For the purpose of the second alternative in Art. 16 para. 1 the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, is mainly based on the following Sections of the Code of Criminal Procedure (CCP):

Seizure

§ 110. (1) A seizure shall be admissible if it appears to be necessary

1. for reasons of evidence,

2. to secure private-law claims, or

3. to secure the skimming off of a confiscation (§ 19a of the Criminal Law Code), an enrichment (§ 20 of the Criminal Law Code), a forfeiture (§ 20b of the Criminal Law Code), a recovery (§ 26 of the Criminal Law Code) or another property-law order stipulated by law.

(2) The public prosecutor shall order a seizure, and the criminal police shall perform it.

(3) The criminal police is entitled to seize objects (§ 109 item 1, letter a) at its own initiative

1. if

a. nobody has disposing power over them,

b. they were taken from the victim as a result the punishable act,

c. they were found on the site of the offence and might have been used to commit the punishable act or might have been intended to commit it, or

d. they are of low value or can be replaced easily on a temporary basis,

2. if their possession is generally prohibited (§ 445a (1)),

3. if a person, who has been arrested for the reason of § 170 (1) item 1, was found with them, or if they were found in the course of a search of that person pursuant to § 120 (1), or

4. in the cases of Article 18 of the Council Regulation (EC) No 608/2013 of 29 June 2013 concerning customs enforcement of intellectual property rights and repealing Council Regulation (EC) No 1383/2003 (Official Journal No. L 181 of 29/06/2013, page 15).

(4) The seizure of objects for reasons of evidence (paragraph (1) item 1) shall not be admissible and shall certainly be lifted upon a request by the person concerned whenever and as soon as the purpose of evidence can be satisfied by video, audio or other recordings, or by copies of written records or data processed with electronic support, and it is not to be assumed that the seized objects as such or the originals of the seized information will have to be viewed during the trial.

§ 111. (1) Every person, who has in his/her disposing power objects or property items that are to be seized, shall be obliged (§ 93 (2)) to release them, when so requested by the criminal police, or to facilitate the seizure in any other way. This obligation may be enforced, if necessary also by way of a search of person or premises, in which context § 119 to § 122 shall be applied in analogy.

(2) If information saved on data carriers is to be seized, everybody shall grant access to the information and hand over or have produced an electronic data carrier in a generally customary data format, when so requested. Moreover, he/she shall suffer the production of a back-up copy of the information saved on the data carriers.

(3) Persons, who themselves are not accused of the offence, shall, upon their application, receive a refund of the reasonable and locally customary costs that they have incurred, of needs, by the handing over documents or other objects of relevance as evidence of third parties, or by handing over copies.

(4) In any event, the person affected by the seizure shall be issued or sent a confirmation of the seizure immediately, or within 24 hours at the latest, and he/she shall be informed of his/her right to file an objection (§ 106). Whenever possible, the victim shall also be informed of a seizure to secure a decision on private-law claims (§ 110 (1) item 2).

[…]

Definitions

§ 117. For the purposes of the present law, the following terms shall mean:

[…]

2. "search of premises and objects" is to search

a. a generally not accessible piece of land, a room, a vehicle or a container,

b. a flat or another location that is protected by domestic authority, as well as the objects located therein,

3. "search of a person" is

a. to search the clothes worn by a person and the objects which the person carries with him/her,

b. to inspect the body of an undressed person,

[…]

Search of Premises and Objects

§ 119. (1) A search of premises and objects (§ 117 item 2) shall be admissible if it is to be expected, on account of certain facts, that a person is hiding there, who is suspected of a punishable act, or that objects or traces are there, which must be secured or processed.

(2) A search of a person (§ 117 item 3) shall be admissible if that person

1. was arrested or caught in the act of committing a punishable act,

2. is suspected of a punishable act and it is to be expected, on account of certain facts, that he/she is carrying objects that are subject to seizure, or that he/she has traces with him/her,

3. might have suffered injuries which are due to a punishable act, or experienced other changes on his/her body, the determination of which is required for the purposes of criminal proceedings.

§ 120. (1) Searches of premises and objects pursuant to § 117 item 2, letter b, and of persons pursuant to § 117 item 3, letter b, shall be ordered by the public prosecutor on the basis of a court authorization; in the case of an imminent danger, the criminal police is entitled, though, to conduct these searches without any order and authorization, for the time being. The same

applies to the cases of § 170 (1) item 1 for the search of persons pursuant to § 117 item 3, letter b. However, a victim must not be forced in any event to be searched against his/her will (§ 119 (2) item 3 and § 121 (1) last sentence).

(2) Searches pursuant to § 117 item 2, letter a, and pursuant to § 117 item 3, letter a, may be conducted by the criminal police on its own initiative.

§ 121. (1) Prior to every search, the person concerned shall be requested, indicating the reasons decisive for the request, to allow the search, or to hand over the sought object voluntarily. This request may only be waived if there is an imminent danger, as well as in the case of § 119 (2) item 1. The use of force (§ 93) shall be inadmissible in the case of searches of persons pursuant to § 119 (2) item 3.

(2) The person concerned has the right to be present at a search pursuant to § 117 item 2, as well as to call in a person of his/her confidence for such a search, as well as for a search pursuant to § 117 item 3, letter b. § 160 (2) shall apply to that person in analogy. If the owner of the flat is not present, another adult co-user of the flat may exercise his/her rights. If this is not possible either, two persons of confidence without any involvement in the matter shall be called in to attend the search. This requirement may only be waived in case of an imminent danger. A representative of the respective statutory professional organization and/or the media owner, or a representative nominated by the latter shall be asked to attend a search of premises used exclusively for the exercise of an occupation by one of the persons listed in § 157 (1) items 2 to 4.

(3) When performing a search attracting attention, causing annoyance and disturbance shall be restricted to the unavoidable minimum. The property and personal rights of all persons concerned shall be safeguarded to the extent possible. A search of persons pursuant to § 117 item 3, letter b, shall always be conducted by a person of the same sex, or by a physician, respecting the dignity of the person to the searched.

§ 122. (1) As soon as possible, the criminal police shall report to the public prosecutor about any search pursuant to § 120 (1) last half-sentence of the first sentence (§ 100 (2) item 2); the criminal police shall then apply to the court for a decision on the admissibility of the search (§ 99 (3)). If the authorization is not granted, the public prosecutor and the criminal police shall apply every legal means at their disposal to restore the legal status corresponding to the court decision.

(2) If objects are found in the course of a search that lead one to conclude that another punishable act has been committed than the one for which the search has been conducted, these objects shall be seized; yet, a separate record shall be drawn up on this process, which shall immediately be reported to the public prosecutor.

(3) In any event, the person concerned shall be handed or sent a confirmation of the search and its result immediately or within 24 hours at the latest, as well as of the order by the public prosecutor and the court decision, if applicable.

2. For the seizure of traffic data it is necessary to investigate them first. The following provisions of the CCP are relevant therefor:

Definitions

§ 134. For the purposes of the present law, the following terms shall mean:
1. "confiscation of letters" relates to telegrams, letters or other mail pieces that are opened or held back, which the accused sends off, or which are addressed to him/her,
2. "information about the data of a message transmission" is information that is provided about communication data (§ 92 (3) item 4 of the Telecommunications Act), access data (§ 92 (3) item 4a of the Telecommunications Act) which is not ordered by § 76a item 2 and position data (§ 92 (3) item 6 of the Telecommunications Act) of a telecommunications service, or a service of the information society (§ 1 (1) item 2 of the Notification Act),
[…]
5. "result" (of the confiscation, information or surveillance listed in items 1 to 4) is the contents of letters (item 1), the data of a message transmission, or the contents of transmitted messages (items 2 and 3), and the image and sound recordings of a surveillance operation (item 4).

Confiscation of Letters, Information about Data of a Message Transmission, as well as Surveillance of Messages

§ 135. (1) The confiscation of letters shall be admissible if it is required to clear up a punishable act, committed with intent, which carries a prison term of more than 1 year, and if the accused is being kept detained for such an act, or if his presentation in court or arrest has been ordered for this purpose.

(2) Information about the data of a message transmission shall be admissible

1. if and as long as it is urgently suspected that one of the persons concerned by the information has kidnapped or otherwise seized another person, and that the information about data is restricted to such a message of which it has to be assumed that it was communicated, received or sent by the accused at the time when the person was deprived of his/her liberty,

2. if it is to be expected that this can promote the clearing up of a punishable act, committed with intent, which carries a prison term of more than six months, and if the owner of the technical equipment, which was or will be the source or the target of a message transmission, expressly agrees to it, or

3. if it is to be expected that this can promote the clearing up of a punishable act, committed with intent, which carries a prison term of more than one year, and if it is to be assumed, on account of certain facts, that data concerning the accused can thus be obtained,

4. if it is to be expected on the basis of certain facts that the whereabout of a volatile or absent person, who is accused of an intentionally committed criminal act with a possible prison term of more than one year, can be detected.

(3) The surveillance of messages shall be admissible

1. in the cases of paragraph (2) item 1,

2. in the cases of paragraph (2) item 2, whenever the owner of the technical equipment, which was or will be the source or target of the message transmission agrees to the surveillance,

3. if this appears to be required to clear up a punishable act, committed with intent, that carries a prison term of more than one year, or if the clearing up or prevention of a punishable act, committed or planned within the framework of a criminal or terrorist association or a criminal organisation (§ 278 to § 278b of the Criminal Law Code) would otherwise be essentially impeded, and

   a. the owner of the technical equipment, which was or will be the source or target of messages is urgently suspected of a punishable act, committed with intent, that carries a prison term of more than one year, or of a punishable act pursuant to § 278 to § 278b of the Criminal Law Code, or

   b. it is to be expected, on account of certain facts, that a person urgently suspected of the offence (letter a) will use the technical equipment or will establish contact with it;

4. in the cases of paragraph 2 item 4.

Common Provisions

§ 137. (1) The criminal police may conduct a surveillance pursuant to § 136 (1) item 1 on its own initiative. The other investigative measures pursuant to § 135 and § 136 shall be ordered by the public prosecutor on the basis of a court authorization, with the entering of rooms pursuant to § 136 (2) always requiring a court authorization in each individual case.

(2) § 111 (4) and § 112 shall be applied in analogy to the confiscation of letters.

(3) Investigative measures pursuant to § 135 and § 136 may only be ordered for such a future period of time (in the cases of § 135 (2) also for such past periods of time) that are likely to be required in order to fulfil the purpose. Another order is admissible in every case, whenever it is to be expected on account of certain facts that the further performance of an investigative measure will lead to success. Moreover, the investigative measure shall be ended as soon as its requirements have ceased to apply.

§ 138. (1) Orders and court authorizations for the confiscation of letters pursuant to § 135 (1) shall indicate the designation of the proceedings, the name of the accused, the offence of which the accused is suspected and its statutory designation, as well as the facts from which it results that the order or the authorization is required and proportional in order to clear up the offence. An order and authorization of an investigative measure pursuant to § 135 (2) and (3), as well as § 136 shall also contain the following:

1. the name or other identification features of the proprietor of the technical device that was or will be the origin or target of a message communication, or of the person whose surveillance is being ordered,

2. the premises envisaged to carry out the investigative measure,

3. the type of message communication, the technical equipment and the terminal device, or the type of the technical means that is likely to be used for the optical and acoustic surveillance,

4. the time when the surveillance begins and ends,

5. the premises which may be entered on the basis of the order,

6. in the case of § 136 (4) the facts from which results the serious danger to public security.

(2) Operators of postal and telegraph services are obliged to cooperate in the confiscation of letters and, upon an order by the public prosecutor, hold back such mailings until a court authorization has been received; if such an authorization is not granted within three days, they must not postpone the delivery any further. Providers (§ 92 (1) item 3 of the Telecommunications Act) and other providers of services (§ 13, § 16 and § 18 (2) of the E-Commerce Act, Federal Law Gazette I No. 152/2001) are obliged to provide information about data of a message transmission (§ 135 (2)) and to cooperate in the surveillance of messages (§ 135 (3)).

(3) The obligation pursuant to paragraph (2) and its scope, as well as a possible obligation to keep confidential facts and processes linked to the order and the authorization shall be imposed upon the provider by the public prosecutor by means of a separate order. This order shall indicate the corresponding court authorization. § 93 (2), § 111 (3), as well as the provisions on searches shall

apply in analogy.

(4) The public prosecutor shall review the results (§ 134 item 5) and have those parts transformed into images or written form, as well as annexed to the files that are of significance for the proceedings and may be used as evidence (§ 140 (1), § 144, § 157 (2)).

(5) After ending an investigative measure pursuant to § 135 (2) and (3), as well as § 136, the public prosecutor shall immediately serve his/her order and the court authorization on the accused and the persons concerned by the investigative measure. However, the service may be postponed for as long as this would jeopardize the purpose of these or other proceedings. If the investigative measure was begun later or ended earlier than at the times indicated in paragraph (1) item 4, the period of the actual performance shall also be communicated.

§ 139. (1) The accused shall be given an opportunity to see and hear all results (§ 134 item 5). Whenever the interests of third parties so require, the public prosecutor shall, however, exclude from becoming known to the accused those parts of the results that are not of significance for the proceedings. The foregoing shall not apply whenever the results are being used during the trial.

(2) The persons concerned by the performance of investigative measures shall have the right to examine the results whenever they relate to their data of a message transmission, to messages addressed to them or sent by them, or to conversations conducted by them, or to images showing them. The public prosecutor shall inform these persons of this right and their right under paragraph (4), to the extent that their identity is known, or can be established without particular effort.

(3) Upon application by the accused, further results in image or written form shall be transformed if this is of significance for the proceedings and their use as evidence is admissible (§ 140 (1), § 144, § 157 (2)).

(4) Upon application by the accused or ex officio the results of the investigative measure shall be destroyed if they cannot be of significance for criminal proceedings, or may not be used as evidence. The persons concerned by the investigative measure also have this right of application, to the extent that these are messages or images showing them, which are addressed to them, or sent by them, or conversations conducted by them.

3. According to Art. 16 para. 3 of the Convention, the confidential treatment of data is in any case ensured since data which was achieved through investigative seizure measures has to be stored first by the police and afterwards by the public prosecutor (§ 114 para. 1 CPC). Therefore such data are only accessible to persons who are sworn to secrecy. The maintaining of confidentiality for service providers follows from § 138 (3) CPC.

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

All types of data are covered, taking into account that content data in the sense of § 134 (3) CCP does not make reference to the past. It is a matter of "real time" data.

Q1.1.3.Do they apply to electronic evidence in relation to any criminal offence or are there limitations? Please explain.

There are no specific rules in the Austrian CCP concerning electronic evidence. Generally all evidence is admissable. At least the court has to decide on the basis of the evidence by free conviction whether facts are noted as proved; in doubt, always in favor of the defendant (§ 14 CCP). Nevertheless the preservation of specified computer data that has been stored by means of a computer system is done with a special software which excludes subsequent data manipulation.

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

According to § 138 (2) CCP operators of postal and telegraph services are obliged to cooperate in the confiscation of letters and, upon an order by the public prosecutor, hold back such mailings until a court authorization has been received; if such an authorization is not granted within three days, they must not postpone the delivery any further. Providers (§ 92 (1) item 3 of the Telecommunications Act) and other providers of services (§ 13, § 16 and § 18 (2) of the E-Commerce Act, Federal Law Gazette I No. 152/2001) are obliged to provide information about data of a message transmission (§ 135 (2)) and to cooperate in the surveillance of messages (§ 135 (3)).

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

The preservation basically is visible to suspects, if the purpose of the investigation does not require otherwise (e.g. concerning the investigation and seizure of data of a message transmission). If the person affected by the seizure or present at the seizure opposes the seizure of written records or data carriers by invoking an obligation to confidentiality recognized by law, these records and data carriers shall be secured in an appropriate form and manner against any unauthorized examination or change, and submitted to the court. They may not be viewed before further steps have been taken. Finally the court shall go through the records and data carriers and decide whether and to what extent they shall continue to be seized or returned to the person concerned. A complaint against this step shall have suspensive effect (§ 112 CCP).

1.2.Procedures

Q1.2.1.Please describe the end-to-end procedure for the handling of a request.

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

1.3.Practical experience

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

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

Q1.3.3 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?

Additional to Q 1.1.1: The criminal investigation department, the public prosecutors office and the court are only allowed to intervene in the rights of persons by procuring evidence as it is expressly provided in law and required to achieve the mission. Any violation of a legally protected interest has to be proportionate to the weight of the offense, the degree of suspicion and the desired success (§ 5 (1) CCP).

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?

Q 1.3.6 Please describe a typical case or scenario.

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

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

2.1.Legislation/regulations

Q2.1.1.What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

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

The relevant provisions can be found in § 94 (1) and (4) Telecommunications Act 2003 and § 138 (2) CCP:

Technical facilities

§ 94. (1) In accordance with the ordinances issued under Par. 3 and 4, the provider shall be obliged to make available all facilities necessary for monitoring communications and for providing information on data in communications, including information on retained data in accordance with the provisions of the Code of Criminal Procedure. For the provision of information, the provider is to be reimbursed 80% of the costs (personnel and material costs) incurred in order to establish the functions necessary pursuant to the ordinances issued under Par. 3 and 4 in the provider's systems. In agreement with the Federal Minister of the Interior, the Federal Minister of Justice and the Federal Minister of Finance, the Federal Minister of Transport, Innovation and Technology shall issue an ordinance defining the assessment base for this percentage and the procedures for asserting such claims to reimbursement. This ordinance shall account, in particular, the economic reasonableness of the effort, any possible interest of the undertaking concerned in the services to be provided and any possible danger caused

by the technical facilities provided which is to be averted by the participation requested, as well as the simplicity and economy of the procedure.

(2) The provider shall be obliged to cooperate to the required extent in the monitoring of communications and in the provision of information on communications data, including information on retained data, in accordance with the provisions of the Code of Criminal Procedure. In agreement with the Federal Minister of Transport, Innovation and Technology and the Federal Minister of Finance, the Federal Minister of Justice shall issue an ordinance providing for adequate compensation of costs, taking into account, in particular, the economic reasonableness of the effort, any possible interest of the undertaking concerned in the services to be provided and any possible danger caused by the technical facilities provided which is to be averted by the participation requested, as well as the public duty of the administration of justice.

(3) By way of ordinance, the Federal Minister of Transport, Innovation and Technology, in agreement with the Federal Ministers of the Interior and Justice, may specify, in line with the state of the art, detailed provisions for the design of the technical facilities to guarantee interception of communications according to the provisions of the Code of Criminal Procedure and for the protection of the data to be transmitted from unauthorised notice or use by third parties. A report shall be submitted to the executive committee of the National Council directly after the ordinance has been issued.

(4) The transmission of traffic data, location data and master data which require the processing of traffic data, including the transmission of retained data, under the provisions of the Code of Criminal Procedure as well as the Security Police Act, must be carried out using a transmission technology which allows the identification of the sender and recipient as well as ensuring data integrity. The data are to be transmitted in comma-separated value (CSV) file format using an advanced encryption technology. This does not apply to the transmission of data in cases pursuant to § 98, of data in cases pursuant to § 99 (5) no. 3 and 4 in cases of imminent danger, of location data in cases requiring determination of current whereabouts pursuant to § 134 et seq. Code of Criminal Procedure, or the transmission of accompanying call data in the course of communications monitoring. In agreement with the Federal Minister of the Interior and the Federal Minister of Justice, the Federal Minister of Transport, Innovation and Technology may issue an ordinance stipulating a standardised definition of the syntax, data fields and encryption for the storage and transmission of the data as well as further specifications regarding storage and transmission of the logs. A report shall be submitted to the executive committee of the National Council directly after the ordinance has been issued.

For § 138 (2) CCP see Q.1.1.1/2.

2.2.Procedures

Q2.2.1 Please describe the end-to-end procedure for the handling of a request.

See Q 1.1.4.

2.3.Practical experience

Q2.3.1.How relevant to investigations in your country is partial disclosure?

Q 2.3.2 How frequently do you use these provisions?

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

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

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

3.1.Legislation/regulations

Q3.1.1.What legal provisions/regulations do you apply for executing an international request for preservation? Please list and attach text.

Q3.1.2 Who has the competence for receiving and executing the international preservation request? What is the role of the contact point?

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

3.2.Procedures

Q3.2.1.Please describe the end-to-end procedure for the handling of the request.

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

Q3.2.3.Other than the information listed in Article 29.2, what information do you need in order to execute a request?

Q3.3. Practical experience

Q3.3.1How frequently do you send and receive international preservation requests? Please provide estimated numbers if readily available.

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

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

Q 3.3.4 Please describe a typical case or scenario.

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

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

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

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

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

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

4.1.Legislation/regulations

Q4.1.1.What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

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

4.2.Procedures

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

4.3.Practical experience

Q 4.3.1 How frequently do you use this provision?

Q.4.3.2.Please describe a typical case or scenario.

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

6.3 Belgium

Belgium does not yet have any legislation transposing the articles 16 and 17 of the convention into Belgian law. There is currently work on a legislative proposal to do so.

Belgium has legislation on data retention since the Bill of 30 July 2013 and the Royal Decree of 19 September 2013. The retention period is one year. The judgment of the European Court of Justice did not have an influence on this legislation so far. However, there is an appeal running against our legislation at the Constitutional Court. The Belgian authorities are waiting for the judgement of the CC and will decide thereafter if Belgian legislation has to be modified.

6.4 Czech Republic

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).

When considering a crime according to the Czech law and committed in Czech jurisdiction, it is firstly necessary to distinguish between traffic and localization data on one side (regulated by the Act on Electronical Communications) and all other data (regulated by the Act on Services for Information Society).

The data regulated by Act on Services for Information Society are accessible using general provisions of the Criminal Proceedings Code (Art. 8 of Act num. 141/1961 Coll.) or Act on Police (Art. 18 of Act num. 273/2008 Coll.).

The data regulated by Act on Electronical Communications are accessible using the provisions of Art. 78 of the Criminal Proceedings Code. Thus they are accessible only if there is a reasonable suspicion of a criminal act and the data is related to it.

Q 1 1 2 Do they cover all types of data (traffic, content) stipulated by article 16?

All types of data are covered, although in different ways.

Q 1 1 3 Do they apply to electronic evidence in relation to any criminal offence or are there limitations? Please explain.

Aforementioned provisions apply when any criminal offence is concerned. There are no exceptions.

Q 1 1 4 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

Because such an agreement would lack legal basis, there exist none. Thanks to the relations between the subjects (either to the Act on Electronical Communications or Act on Services for information society) no arrangement (eg. on their joint representation) was ever reached.

Q 1 1 5 Is preservation visible to the suspects or account holder or can you prevent disclosure of the preservation request?

In case provisions on eavesdropping are used (in case of continual traffic monitoring) and in case traffic and localization data are monitored, the subject must be notified after the eavesdropping has ended according to Art. 88 of the Criminal Proceedings Code.

1.2.Procedures

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

A) In case of data regulated by the Act on Electronical Communications:
A police department finds reasonable suspicion of a committed crime. It gives the information to a prosecutor, who files a warrant to the subject to preserve and hand in the data. Then the data is preserved and handed in to the police department.

B) In case of data regulated by the Act on Services for Information Society:
A police department finds a need to fulfill its tasks. A request is sent by the police department to the subject who is obliged to fulfill the request.

Q 1. 2. 2 What templates/forms are used? Please attach if any.

No templates/forms are 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?

Expedited preservation is executed on the basis of general provisions. Missing these general provisions would create severe problems for law enforcement.

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

Exceptionally thanks to the limitations listed above.

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?

It is not specifically foreseen.

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

Yes

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

The providers seem ready to cooperate if a specific legal basis for the issue exists.

Q 1.3.6 Please describe a typical case or scenario.

The department is notified that an e-mail threatening with an explosive device was sent via an anonymizing service located in the Czech Republic. Further lead to the identity of the writer is requested. Such a request often comes from other countries than the Czech Republic. In these cases an e-mail from a previously verified address is most common.
Because this kind of data falls under the Act on Services for Information Society, it is relatively easy to reach and typically it is a matter of days until the data is handed over to the requesting party (be it other Police Department or foreign Police Office).

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

As described above, the lack of specific regulation brings issues with regard to procedure and thus with the ability to reach the desired data effectively.

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

2.1.Legislation/regulations

Q2.1.1.What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

Thanks to the absence of specific regulation, the general regulation as described above applies.

Q2.1.2 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

There exist no arrangements.

2.2.Procedures

Q2.2.1.Please describe the end-to-end procedure for the handling of a request.

Thanks to the absence of specific regulation, the procedure is the same as described above.

2.3.Practical experience

Q2.3.1.How relevant to investigations in your country is partial disclosure?

Thanks to is sparse use it is not essential.

Q2.3.2.How frequently do you use these provisions?

Rarely

Q2.3.3.In general, what is the response time by service providers

According to the type of data requested and the ability of the subject to react it may take from minutes to days.

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

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

3.1.Legislation/regulations

Q3.1.1.What legal provisions/regulations do you apply for executing an international request for preservation? Please list and attach text.

National legislation please see above (mainly answer 1.1.1). The cooperation is initiated mainly on the basis of the Convention on Cybercrime.

Q3.1.2.Who has the competence for receiving and executing the international preservation request? What is the role of the contact point?

The contact point is Police Presidium of the Czech Republic, Bureau of Criminal Police and Investigation Service, Information Technology Crime Section. In this case the role of the Section is to be a 24/7 contact point, generally it is a central police office for directing and coordinating fight against cybernetic crime.

Q 3.1.3 What rules apply for the transfer of the data preserved to foreign authorities?
Usual rules concerning MLA would apply for the transfer of data.

If the data is not under specific protection as described in the text above, then the request is directly answered. If there is a specific protection, MLA request is necessary.

3.2.Procedures

Q3.2.1.Please describe the end-to-end procedure for the handling of the request.

As described in answer 1.2.1.

Q3.2.2.What templates/forms are used for international requests? Please attach if any.

No templates are used.

Q3.2.3.Other than the information listed in Article 29.2, what information do you need in order to execute a request?

The description of a connection between the requested data and the deed prosecuted.

3.3.Practical experience
Q3.3.1How frequently do you send and receive international preservation requests? Please provide estimated numbers if readily available.

Request by the Czech Republic are in single digits and requests addressed to the Czech Republic are in double digits per annum.

Q3.3.2.In general, as a requested country, how quickly do you issue a preservation request?

According to the type of data requested and the ability of the subject to react it may take from minutes to days.

Q3.3.3.In general, as a requesting country, how quickly are you notified that your request has been issued in the foreign country?

Thanks to the limited number of requests it is difficult to generalize.

Q3.3.4.Please describe a typical case or scenario.

As outlined in 1.3.6.

Q3.3.5.Without provisions on preservation, would this create problems for international cooperation?

There are no specific provisions on data preservation in the Czech legislature.

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

The data is not available.

Q3.3.7 How often do you send international preservation requests and not follow them with mutual legal assistance requests or notifications?

Only in case of data could be requested also in the Czech Republic without a warrant.

Q3.3.8.In conclusion: What are the main strengths and what are the main problems of preservation within the framework of international cooperation?

Most of the complications are caused by the differences between the legal systems of different countries.

A good practice that would be desirable in cooperation with more countries is notification about an arrived request. After a request is received, the requested party notifies the requesting party, that the request was received in the matter of hours. This provides the requesting party the knowledge, that the message reached its destination, that it is well enough understood and that it doesn't lack any critical information.

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

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

4.1.Legislation/regulations

Q4.1.1 What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

National legislation please see above (mainly answer 2.1.1). The cooperation is initiated mainly on the basis of the Convention on Cybercrime.

Q4.1.2.What are the conditions, limitations or impediments to disclosing a sufficient amount of traffic data?

Please see answer 2.1.1.

4.2.Procedures

Q4.2.1Please describe the end-to-end procedure for the handling of a request.

As described in answer 2.2.1.

4.3.Practical experience

Q4.3.1 How frequently do you use this provision?

Exceptionally thanks to the limitations listed above.

Q4.3.2.Please describe a typical case or scenario.

As outlined in 1.3.6.

Q4.3.3.Without provisions on partial disclosure, would this create problems for international cooperation?

There are no specific provisions for partial disclosure.

6.5 Denmark

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).

Rule of law

Expedited preservation of stored computer data and traffic data, as well as partial disclosure of traffic data, is regulated by sections 786a and 804 of the Administration of Justice Act:

"The Administration of Justice Act Section 786a.

(1) In connection with an investigation in which electronic evidence may be of importance, the police may impose orders on providers of telecom networks or services to arrange for emergency protection of electronic data, including traffic data.

(2) An order of emergency protection under subsection (1) above may solely comprise electronic data stored at the point in time when the order is imposed. The order must state the data that must be secured and the period for which they must be secured (the period of protection). The order must be limited to comprise solely the data estimated to be necessary for investigation and the protection period must be as short as possible and no more than 90 days. An order of this nature may not be extended.

(3) Providers of telecom networks or services are responsible for ensuring as part of the protection under subsection (1) without undue delay that they pass on traffic data concerning other telecom network or service providers whose networks or services have been used in connection with the electronic communication that may be of importance for the investigation.

(4) Violation of subsections (1) and (3) above is punishable by a fine."

"The Administration of Justice Act Section 804.

(1) In connection with the investigation of an offence which is subject to public prosecution or a case of violation of an order as referred to in section 2(1) para. 1 of the Act on Restraining, Exclusion and Removal Orders, a person who is not a suspect may be ordered to produce or hand over objects (discovery), if there is reason to presume that an object of which that person has the disposal may serve as evidence, should be confiscated or, by the offence, has been procured from someone who is entitled to claim it back. When an order is imposed on a business enterprise, section 189 shall apply correspondingly to others who have gained insight into the case due to their association with the enterprise.

(2) If an object has been handed over to the police following an order of discovery, the rules of seizure according to section 803(1) shall apply correspondingly.

(3) If, without any order to this effect, an object has been handed over to the police for the reasons mentioned in subsection (1) above, section 807(5) shall apply. If a request for return of an object is made, and the police do not grant the request, the police shall as soon as possible and within 24hours submit the case to the court with a request for a seizure order. In that case section 806(4), 2nd sentence, and subsection (6) 1st sentence, shall apply.

(4) An order of discovery may not be issued if it will produce information on matters about which the individual would be exempted from testifying as a witness according to sections 169-172.
(5) The Minister of Justice may issue rules on financial compensation in special cases for costs relating to the fulfilment of an order for discovery."

Q 1 1 2 Do they cover all types of data (traffic, content) stipulated by article 16?

Sections 786a and 804 of the Administration of Justice Act cover all kinds of electronic data.

Q 1 1 3 Do they apply to electronic evidence in relation to any criminal offence or are there limitations? Please explain.

Sections 786a and 804 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?

The Danish Police and the service providers cooperate on the basis of informal agreements as to templates and exchange of information etc. according to the Act on Electronic Communications Networks and Services. Cooperation with other private sector holders of data is agreed upon on a case-by-case basis of mutual cooperation.

Q 1 1 5 Is preservation visible to the suspects or account holder or can you prevent disclosure of the preservation request?

Telecommunications networks and service providers are subject to rules of confidentiality.

According to section 7 of the Act on Electronic Communications Networks and Services the owners and providers of electronic communications networks or services and the employees and former employees may not unjustifiably forward or take advantage of information that they have obtained through their involvement in the networks or services about others' use of the networks or services.

The sections on penalty for breach of confidentiality in the Criminal Code are equally applicable to persons who are employed or have been employed by an owner of a provider of electronic communications network or service or a person that carry out tasks for such a network or service provider.

This framework on confidentiality is, inter alia, applicable in cases where police expeditiously order providers of telecommunications networks or services to preserve data.

1.2.Procedures

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

The police request the service provider or others to preserve the data.

Q 1. 2. 2 What templates/forms are used? Please attach if any.

No specific templates are used for the request of preservation.

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?

Expedited preservation is seldom used in Denmark compared to the other available measures in the Administration of Justice Act. However, when the Danish police investigate criminal cases on the basis of information received late from international partners, expedited preservation is useful.

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

No statistical information is available, but they are seldom used.

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?

Expedited preservation is specifically foreseen in respect of providers of telecom networks or services. In case preservation is needed in respect of others, e.g. banks, the general rules on production orders will be applied (section 804).

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

Yes, in accordance with the general rules on production orders, as the specific rules on expedited preservation apply only to providers of telecom networks or services.

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

Well-functioning and cooperative.

Q 1.3.6 Please describe a typical case or scenario.

Through well-established informal or formal networks the police request the service provider or others to preserve electronic data. Typically, the prosecution service files for a warrant for discovery of evidence in accordance with section 804 of the Administration of Justice Act or a warrant for search or seizure.

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

See above answers.

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

2.1.Legislation/regulations

Q2.1.1.What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

See answer to Q 1.1.1.

Q2.1.2 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

The Danish Police and the service providers cooperate on basis of informal agreements as to templates and exchange of information etc. according to the Danish act on Electronic Communications Networks and Services.

2.2.Procedures

Q2.2.1.Please describe the end-to-end procedure for the handling of a request.

The police request the service provider or others to preserve the data.

2.3.Practical experience

Q2.3.1.How relevant to investigations in your country is partial disclosure?

The possibility is hardly ever used.

Q2.3.2.How frequently do you use these provisions?

No statistical information is available, but they are seldom used.

Q2.3.3.In general, what is the response time by service providers

A few hours or less.

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

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

3.1.Legislation/regulations

Q3.1.1.What legal provisions/regulations do you apply for executing an international request for preservation? Please list and attach text.

There is no specific Danish legislation relating to mutual legal assistance in criminal matters. In all cases where assistance from Denmark is required, including a request for preservation, the
Danish authorities apply national legislation by analogy. This implies that Danish authorities can comply with requests for mutual legal assistance even though no bilateral or multilateral agreement exists between Denmark and the requesting country. This also implies that Danish authorities can comply with a request if the investigative measure(s) covered by the request could be carried out in a similar national case. Therefore, requests are executed in accordance with national law, i.e. the Administration of Justice Act, and – if applicable - in accordance with relevant international

instruments such as the 1959 European Convention on Mutual Legal Assistance in Criminal Matters and the 2001 Convention on Cybercrime.

Reference can consequently be made to the answer to Q 1.1.1.

Q3.1.2.Who has the competence for receiving and executing the international preservation request? What is the role of the contact point?

The Ministry of Justice is in accordance with Article 27, paragraph 2, of the 2001 Convention on Cybercrime designated as the central authority for sending and receiving requests for mutual legal assistance, including preservation requests. Requests sent on the basis of the 2000 Convention on Mutual Assistance in Criminal Matters between Member States of the European Union are generally transmitted directly between judicial authorities.

Requests are executed where appropriate by one or more authorities, e.g. the Danish State Prosecutor for Serious Economic and International Crime, the police, the Prosecution Service, the courts etc.

Q 3.1.3 What rules apply for the transfer of the data preserved to foreign authorities?
Usual rules concerning MLA would apply for the transfer of data.

The national rules regarding transfer and disclosure of data apply by analogy to the transfer of preserved data to foreign authorities. Data can be disclosed or transferred to a foreign authority as long as the disclosure/transfer fulfills the same conditions as in a similar national case.

3.2.Procedures

Q3.2.1.Please describe the end-to-end procedure for the handling of the request.

The powers to secure electronic evidence through preservation in an expedited manner at the domestic level are also applied for international requests. Requests are received at a 24/7 single contact point at the Danish National Police by e-mail. Receipt is confirmed. A request is sent by the Danish National Police to the service provider or others. Upon reply by the service provider or others the requesting contact point is informed and depending on the circumstances asked to forward a request of mutual legal assistance in order to obtain the data.

Q3.2.2.What templates/forms are used for international requests? Please attach if any.

No specific form is used.

Q3.2.3.Other than the information listed in Article 29.2, what information do you need in order to execute a request?

None

3.3.Practical experience

Q3.3.1How frequently do you send and receive international preservation requests? Please provide estimated numbers if readily available.

No statistical information is available.

Q3.3.2.In general, as a requested country, how quickly do you issue a preservation request?

Within hours.

Q3.3.3.In general, as a requesting country, how quickly are you notified that your request has been issued in the foreign country?

It varies from a few hours until several days.

Q3.3.4.Please describe a typical case or scenario.

There is no typical scenario, but when requesting expeditious preservation the suspected crime committed could, inter alia, be a case of sexual abuse of children or of economic crime.

Q3.3.5.Without provisions on preservation, would this create problems for international cooperation?

Yes.

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

No statistical information is available.

Q3.3.7 How often do you send international preservation requests and not follow them with mutual legal assistance requests or notifications?

Seldom.

Q3.3.8.In conclusion: What are the main strengths and what are the main problems of preservation within the framework of international cooperation?

The time it takes before the foreign country responds may in some cases be a problem.

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

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

4.1.Legislation/regulations

Q4.1.1 What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

See answers to Q 3.1.1. and Q 1.1.1.

Q4.1.2.What are the conditions, limitations or impediments to disclosing a sufficient amount of traffic data?

See answer to Q 3.1.3.

4.2.Procedures

Q4.2.1Please describe the end-to-end procedure for the handling of a request.

Information to the requesting state containing sufficient amount of traffic data to identify a service provider in a third state is forwarded without delay through the single contact point atthe Danish National Police.

4.3.Practical experience

Q4.3.1 How frequently do you use this provision?

No statistical information is available.

Q4.3.2.Please describe a typical case or scenario.

There is no typical scenario, but when requesting expedited disclosure of preserved traffic data the suspected crime committed could, inter alia, be a case of sexual abuse of children, of drug trafficking or of economic crime.

Q4.3.3.Without provisions on partial disclosure, would this create problems for international cooperation?

It probably would.

6.6 Dominican Republic

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

1.1.Legislation/regulations

Q1.1.1 What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

Law 53-07, Articles 54, 56, 58 (see attached law – in spanish)

Artículo 53.- Conservación de los Datos. Las autoridades competentes actuarán con la celeridad requerida para conservar los datos contenidos en un sistema de información o sus componentes, o los datos de tráfico del sistema, principalmente cuando éstos sean vulnerables a su pérdida o modificación.

Artículo 54.- Facultades del Ministerio Público. Previo cumplimiento de las formalidades dispuestas en el Código Procesal Penal, el Ministerio Público, quien podrá auxiliarse de una o más de las siguientes personas: organismos de investigación del Estado, tales como el Departamento de Investigación de Crímenes y Delitos de Alta Tecnología (DICAT) de la Policía Nacional; la División de Investigación de Delitos Informáticos (DIDI) del Departamento Nacional de Investigaciones; peritos; instituciones públicas o privadas, u otra autoridad competente, tendrá la facultad de:

b) Ordenar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos;

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

Yes.

Q1.1.3.Do they apply to electronic evidence in relation to any criminal offence or are there limitations? Please explain.

Yes, any offence.

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

No formal agreements, just what is in the legislation.

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

There's no specification about disclosure in our legislation, but our ISP's have never notified their customers.

1.2.Procedures

Q1.2.1.Please describe the end-to-end procedure for the handling of a request.

The request for information is made to the service provider by the Prosecutor's office, which in turn handles the request and delivers us an answer to that request.

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

No templates/forms, a simple letter from a prosecutor (or the Police – DICAT – in case of emergencies).

See attached sample

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?

So far, we haven't used the expedited preservation provision with the local IPS's, because the procedure for formally requesting the information is normally very quick (1 or 2 days) and there's a mandatory 90-day preservation period for all data.

On the other hand, with foreign ISP's we have used it, because formally obtaining the data is very complicated (often impossible).

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

Locally: never so far
Internationally: About 20 per year

Q1.3.3 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?

It is foreseen in procedural law, and a preservation letter from a prosecutor or DICAT suffices.

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

It is foreseen in Law 53-07, but never used so far.

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

It is usually very good, we have very good partnerships with the local providers

Q 1.3.6 Please describe a typical case or scenario.

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

The strength is that regulators tell them to preserve the information. The weakness is that time is short related to the time it takes to process the application.

2.Article 17 – Expedited preservation and partial disclosure of traffic data (domestic level) 2.1.Legislation/regulations Q2.1.1.What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

Law 53-07, Article 54 (see attached law – in spanish)

After ruling TC/200-13 of our Constitutional Court the only way to obtain disclosure of any subscriber, traffic or content data from a provider is with a court order. Before this ruling all was needed was a letter from a prosecutor.

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

No formal agreements, just what is in the legislation.

2.2.Procedures

Q2.2.1 Please describe the end-to-end procedure for the handling of a request.

The request for information is made to the service provider by the Prosecutor's office, which in turn handles the request and delivers us an answer to that request.

2.3.Practical experience

Q2.3.1.How relevant to investigations in your country is partial disclosure?

Time is essential in cybercrime investigations, but it's not possible anymore.

Q 2.3.2 How frequently do you use these provisions?

It used to be very often, but not possible anymore after ruling TC/200-13

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

In average, 5 to 7 working days (except for emergency cases).

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

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

3.1.Legislation/regulations

Q3.1.1.What legal provisions/regulations do you apply for executing an international request for preservation? Please list and attach text.

Our law does not extend to international providers, however we make use of the Budapest Convention for such requests.

Q3.1.2 Who has the competence for receiving and executing the international preservation request? What is the role of the contact point?

Artículo 41.- Relaciones Interinstitucionales del DICAT. El DICAT deberá:

a) Trabajar en coordinación con la Comisión Interinstitucional contra Crímenes y Delitos de Alta Tecnología creada por esta ley;

b) Ser el punto de contacto oficial de República Dominicana en la Red Internacional 24/7 de Asistencia en Crímenes que Involucran Alta Tecnología perteneciente al Subgrupo de Crímenes de Alta Tecnología del Grupo de Expertos en Crimen Organizado Transnacional G8; y,

c) Trabajar en coordinación con los demás organismos nacionales

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

Should be done formally through the Attorney General's Office

3.2.Procedures

Q3.2.1.Please describe the end-to-end procedure for the handling of the request.

The request for information is made to the service provider by the Attorney General's Office and Department of Investigation of Crimes and Crimes High Technology (DICAT), which in turn handles the request and delivers us an answer to that request.

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

View attached document

Q3.2.3.Other than the information listed in Article 29.2, what information do you need in order to execute a request?

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

3. *the stored computer data to be preserved and its relationship to the offence;*

4. *any available information identifying the custodian of the stored computer data or the location of the computer system;*

5. *and the necessity of the preservation.*

Q3.3. Practical experience

Q3.3.1How frequently do you send and receive international preservation requests? Please provide estimated numbers if readily available.

Very often we receive requests for preservation of information

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

We process in the same time that we process national requests.

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

We hardly ever get a reply, let alone issue notifications.

Q 3.3.4 Please describe a typical case or scenario.

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

It is necessary the disposition of preservation in order to provide international response.

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

Rarely has not been possible to process an application for preservation of information.

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

Often we do not receive cooperation of our request preservation of information.

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

Our main weakness is because we do not have proper international cooperation for the preservation and delivery of information

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

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

4.1.Legislation/regulations

Q4.1.1.What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

Our law does not extend to international providers, however we make use of budapest agreement for such applications.

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

It depends of the antiquity of the data.

4.2.Procedures

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

The request for information is made to the service provider by the Attorney General's Office and Department of Investigation of Crimes and Crimes High Technology, which in turn handles the request and delivers us an answer to that request.

4.3.Practical experience

Q 4.3.1 How frequently do you use this provision?

Often we use this provision, but only in a few case we have successfully responses.

Q.4.3.2.Please describe a typical case or scenario.

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

We already have limitation to obtain international cooperation, however we often provide opportune information to international request.

6.7 Iceland

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).

In paragraph 47 in the **Communications Act** 81/2003 it is stated (in Icelandic):
Í þágu rannsóknar máls er lögreglu heimilt að leggja fyrir fjarskiptafyrirtæki að varðveita þegar í stað tölvugögn, þar með talin gögn um tölvusamskipti. Fyrirmæli lögreglu geta eingöngu tekið til gagna sem þegar eru fyrir hendi. Í fyrirmælunum á að koma fram hvaða gögn eigi að varðveita og hve lengi, en sá tími má þó ekki vera lengri en 90 dagar.
Unofficial English translation: The police may in the process of an investigation order a telecommunication company to preserve immediately computer data, including traffic data. The order of the police may only apply to already existing data. The order shall prescribe which data to preserve and for how long, this time may however not exceed 90 days.

Q 1 1 2 Do they cover all types of data (traffic, content) stipulated by article 16?

Yes

Q 1 1 3 Do they apply to electronic evidence in relation to any criminal offence or are there limitations? Please explain.

There are no specific limitations

Q 1 1 4 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

No special agreements or arrangements exist between law enforcement and service providers for expedited preservation of computer data. Informal arrangements are in place for how to exchange computer data if required.

Q 1 1 5 Is preservation visible to the suspects or account holder or can you prevent disclosure of the preservation request?

There is no legal requirement for disclosing preservation to suspects or account holders. If the police, however, gains access to the preserved data at a later stage, then it has a duty to inform in accordance with paragraph 85 of the Act 88/2008 on criminal proceedings.

1.2 Procedures

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

A request would be sent to the police in the respective district, which in turn would contact the service provider(s). If, however, the request would involve a serious incident such as an act of terrorism, then the request would be dealt with by the National Commissioner of the Police.

Q.1. 2. 2 What templates/forms are used? Please attach if any.

No specific templates/forms are 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?

Expedited preservation is not known to have been used in Iceland so far, existing legal measures such as seizure have been used instead. Not using preservation has so far not caused a problem, this could however change with rapid growth in cyber crime.

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

The provision has not been used so far.

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?

Preservation is specifically foreseen in the procedural law.

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

No preservation requests have been served so far.

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

No experience of cooperation yet.

Q 1.3.6 Please describe a typical case or scenario.

Not applicable since this provision has not been used.

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

The system has not been used so far, the lack of experience of practical use is the probably the main problem.

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

2.1.Legislation/regulations

Q2.1.1.What legal provisions do you apply? Please list and attach text. Please also describe and attach internal implementing regulations or instructions (if any).

In paragraph 42 in the Communications Act 81/2003 it is stated (in Icelandic): *Þrátt fyrir ákvæði 1. og 2. mgr. skulu fjarskiptafyrirtæki, í þágu rannsókna sakamála og almannaöryggis, varðveita lágmarksskráningu gagna um fjarskiptaumferð notenda í sex mánuði. Lágmarksskráningin skal tryggja að fjarskiptafyrirtæki geti upplýst hver af viðskiptavinum þess var notandi tiltekins símanúmers, IP-tölu eða notandanafns, jafnframt því að upplýsa um allar tengingar sem notandinn hefur gert, dagsetningar þeirra, hverjum var tengst og magn gagnaflutnings til viðkomandi notanda. Fjarskiptafyrirtæki skal tryggja vörslu framangreindra gagna og er óheimilt að nota eða afhenda umræddar upplýsingar öðrum en lögreglu eða ákæruvaldi í samræmi við ákvæði 3. mgr. 47. gr. Eyða ber umferðargögnunum að þessum tíma liðnum enda sé ekki þörf fyrir þau á grundvelli 2. mgr.*
This paragraph requires service providers to store for 6 months for possible use in a criminal investigation sufficient amount of traffic data, subject to certain requirements, in order so that a user can be identified as well as the connections made.
In paragraph 47 in the Communications Act 81/2003 it is stated (in Icelandic):
Ekki má án undangengins dómsúrskurðar heimila óviðkomandi aðilum að sjá skeyti, önnur skjöl eða annála um sendingar sem um fjarskiptavirkin fara eða hlusta á fjarskiptasamtöl eða hljóðrita þau. Fjarskiptafyrirtæki er þó rétt og skylt að veita lögreglu, í þágu rannsóknar sakamáls, upplýsingar um hver sé skráður eigandi ákveðins símanúmers og/eða eigandi eða notandi vistfangs (IP-tölu). Um aðgang lögreglu að upplýsingum um fjarskipti skal að öðru leyti fara samkvæmt lögum um meðferð sakamála.
This paragraph states that a court order is required to access communication data, but gives an exception that requires service providers to provide the police, as a part of a criminal investigation, sufficient communication data to enable to police to identify the registered owner or user of a telephone number or an IP address. Concerning access of the police to communication data there is also a reference to a more generic law on criminal proceedings.

Q2.1.2 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

No special agreements or arrangements exist between law enforcement and service providers for expedited preservation of computer data. Informal arrangements are in place for how to exchange computer data if required.

2.2.Procedures

Q2.2.1.Please describe the end-to-end procedure for the handling of a request.

Police in the district investigating the case would contact the service provider on the legal basis described in the answer to Q 2.1.1

2.3.Practical experience

Q2.3.1.How relevant to investigations in your country is partial disclosure?

Partial disclosure has not been used in practice so there is no practical experience yet.

Q2.3.2.How frequently do you use these provisions?

They have not been used yet.

Q2.3.3.In general, what is the response time by service providers?

Not applicable.

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

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

3.1.Legislation/regulations

Q3.1.1.What legal provisions/regulations do you apply for executing an international request for preservation? Please list and attach text.

It can be assumed that the request is related to an offence that would be considered a criminal offence in Iceland as dual criminality would be a requirement for responding to the subsequent request for mutual assistance. Then the case could proceed as international police cooperation on a criminal case and the domestic part dealt with according to article 16. In article 22 of the Extradition of Criminals and Other Assistance in Criminal Proceedings Act No. 13, 17th April 1984 it is stated that in order to gather evidence for use in criminal proceedings in another state, it may be decided, in response to a request, that the provisions of the (Code of Criminal Procedure) shall be applied in the same manner as in comparable proceedings in Iceland. Requests based on the Cybercrime Convention and the European Convention on Mutual Assistance in Criminal Matters from 29 May 2000 and the protocol thereto from 16 October 2001 shall therefore be executed on that legal basis.
An English translation of the Act can be found at:
http://eng.innanrikisraduneyti.is/laws-and-regulations/english/extradition-and-other-assistance/

Q3.1.2.Who has the competence for receiving and executing the international preservation request? What is the role of the contact point?

In accordance with Article 35 of the Convention, the Government of Iceland has designated as the point of contact available on a 24 hours, 7 days per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence:
National Commissioner of the Icelandic Police

Q 3.1.3 What rules apply for the transfer of the data preserved to foreign authorities?
Usual rules concerning MLA would apply for the transfer of data.

3.2.Procedures

Q3.2.1.Please describe the end-to-end procedure for the handling of the request.

The request would be sent to the official point of contact in Iceland, the National Commissioner of the Icelandic Police, which would in turn forward the request to the police in the respective district, which in turn would contact the service provider(s) as explained in the answer to Q 1.2.1 regarding article 16.

Q3.2.2.What templates/forms are used for international requests? Please attach if any.

No specific templates/forms are used.

Q3.2.3.Other than the information listed in Article 29.2, what information do you need in order to execute a request?

It is not foreseen at present that further information would be needed.

3.3.Practical experience
Q3.3.1.How frequently do you send and receive international preservation requests? Please provide estimated numbers if readily available.

We are not aware of any international preservation requests so far.

Q3.3.2.In general, as a requested country, how quickly do you issue a preservation request?

Not applicable since no preservation requests have been made.

Q3.3.3.In general, as a requesting country, how quickly are you notified that your request has been issued in the foreign country?

Not applicable since no requests have been made to a foreign country.

Q3.3.4.Please describe a typical case or scenario.

Not applicable

Q3.3.5.Without provisions on preservation, would this create problems for international cooperation?

So far it seems not, this could however change with rapid growth in cyber crime.

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

Not applicable

Q3.3.7 How often do you send international preservation requests and not follow them with mutual legal assistance requests or notifications?

Not applicable

Q3.3.8.In conclusion: What are the main strengths and what are the main problems of preservation within the framework of international cooperation?

Preservation is regarded as a potentially useful tool, even though it has not been used so far.

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

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

4.1.Legislation/regulations

Q4.1.1 What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

The basis for the international part of the cooperation would be same as described in the answer to Q 3.1.1 and the basis for the domestic part would be as described in the answer to Q 2.1.1.

Q4.1.2.What are the conditions, limitations or impediments to disclosing a sufficient amount of traffic data?

Due to the dual criminality requirement the amount of data disclosed would have to be regarded as appropriate for the level of investigation.

4.2.Procedures

Q4.2.1Please describe the end-to-end procedure for the handling of a request.

Similarly as in the answer to Q 3.2.1, the request would be sent to the official point of contact in Iceland, the National Commissioner of the Icelandic Police, which would in turn forward the request to the police in the respective district, which in turn would contact the service provider(s) as explained in the answer to Q 1.2.1 regarding article 16.

4.3.Practical experience

Q4.3.1 How frequently do you use this provision?

This provision has not been used so far in / by Iceland.

Q4.3.2.Please describe a typical case or scenario.

Not applicable since provision has not been used in Iceland.

Q4.3.3.Without provisions on partial disclosure, would this create problems for international cooperation?

So far it seems not to have created problems, this could however change with rapid growth in cyber crime.

6.8 Japan

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).

- Art. 218 (search and seizure) and Art. 197(3) (preservation request) of the Code of Criminal Procedure with respect to Art. 16(1) of the Convention
- Art. 197(3) (preservation request) and Art. 197(4) (extension of preservation period) of the Code of Criminal Procedure with respect to Art. 16(2) of the Convention
- Art. 197(5) (request for confidentiality) of the Code of Criminal Procedure with respect to Art. 16(3) of the Convention

Code of Criminal Procedure
Article 218
(1) A public prosecutor, a public prosecutor's assistant officer or a judicial police official may, if necessary for investigation of an offense, conduct search, seizure or inspection upon a warrant issued by a judge. In such cases, the inspection and examination of a person shall be conducted upon a warrant for physical examination.
(2) [*Translation is not available for this provision. It is a new provision as a result of the amendment in 2011. In summary, Art. 218 (2) provides that, when there is a need to seize a computer, electronic data from the electronic device (e.g. server) connected to the said computer may be copied to the computer or another electronic media and may be seized.]*
(3) […]

Art. 197
[*Translation is not available for this provision. In summary, Art. 197 (3) provides that, when there is a need to seize certain electronic data, a public prosecutor, a public prosecutor's assistant officer or a judicial police official may request in writing the service providers or persons/entities with local network facility not to delete the necessary traffic record of such data for no more than 30 days. The preservation request must be withdrawn when it becomes clear that seizure of such data is not necessary. Art. 197 (4) provides that preservation period can be extended for no more than 30 days but the total preservation period cannot exceed 60 days. Art. 197 (5) provides that, if necessary, authorities may also request not to disclose information related to the preservation request without good reason.*]

Q 1 1 2 Do they cover all types of data (traffic, content) stipulated by article 16?

Provisions mentioned above cover any recording media in which any types of data mentioned in Article 16 are recorded and/or saved.

Q 1 1 3 Do they apply to electronic evidence in relation to any criminal offence or are there limitations? Please explain.

They apply to electronic evidence in relation to any criminal offences.

Q 1 1 4 What agreements or voluntary arrangements exist between law enforcement and service providers or other private sector holders of data?

With respect to some service providers, the Police applies the procedure specified by respective providers, such as pre-notification of seizure of computer data.

Q 1 1 5 Is preservation visible to the suspects or account holder or can you prevent disclosure of the preservation request?

Preservation of traffic data is generally invisible to the suspects or account holders. Furthermore, pursuant to Art. 197(5) of the Code of Criminal Procedure, authorities can request a service provider and other private sector holding relevant data to maintain the confidentiality of the preservation request.

On the other hand, when preservation is done through search and seizure pursuant to Art. 218 of the Criminal Procedure Code, a warrant must be shown to the person subject to such measure.

Code of Criminal Procedure

Article 110

The search warrant or seizure warrant shall be shown to the person who is to undergo the measure.

Article 222

(1) The provisions of Articles 99, 100, 102 to 105, 110 to 112, 114, 115 and 118 to 124 shall apply mutatis mutandis to the search and seizure conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Articles 218, 220 and 221. The provisions of Articles 110, 112, 114, 118, 129, 131 and 137 to 140 shall apply mutatis mutandis to the inspection conducted by a public prosecutor, public prosecutor's assistant officer or a judicial police official pursuant to the provisions of Article 218 or 220; provided, however, that the dispositions prescribed in Articles 122 to 124 shall not be executed by a judicial constable.

[…]

1.3 Procedures

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

(5) Investigating authorities specify the computer data necessary for investigation and the holder(s) of such data.
(6) Public prosecutor, public prosecutor's assistant officer or a judicial police official (hereinafter referred to as "investigating officials") drafts the preservation request document and sends it to the data holder [for traffic data only].
(7) Investigating officials request for issuance of a seizure warrant to a judge and receive the warrant.
(8) Investigating officials show the seizure warrant to the data holder (service provider) and seize the data specified in the warrant upon submission by the holder.

Q 1. 2. 2 What templates/forms are used? Please attach if any.

As attached, we use forms for preservation request, withdrawal of preservation request, notification of extension of preservation request period and application for seizure warrant.

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?

Expedited preservation of traffic data necessary for investigation is important as traffic data plays a crucial role in identifying a suspect in the course of cybercrime investigation and yet, traffic data are often erased after a short period of time in general.

In Japan, preservation of traffic data is done expeditiously pursuant to Art. 197 of the Code of Criminal Procedure. A preservation request pursuant to Art. 197 may be carried out without a warrant issued by a judge, unlike a search or a seizure.

Please note that, in Japan, preservation of computer data other than traffic data is done through seizure promptly upon issuance of a warrant by a judge pursuant to Art. 218 of the Code of Criminal Procedure. Since the Japanese judges usually issue a seizure warrant in 1 day, the requirement for a warrant has not posed any obstacles to an investigation up until now.

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

In 2013 (Jan-Dec), the total number of preservation requests for traffic data was 233 (the data combines the requests made by all the investigating authorities, including prosecution and police).

With respect to seizures of computer data other than traffic data pursuant to Art. 218 of the Code of Criminal Procedure, we have no statistics.

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?

It is specifically foreseen in the Code of Criminal Procedure (please refer to Q1.1.1).

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

It is legally possible to serve preservation requests of traffic data to natural or legal persons other than service providers under Art. 197(3) of the Code of Criminal Procedure. In addition to commercial service providers, under this provision, entities such as corporations, public offices and universities with LAN are included as potential subject of the preservation requests.

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

They are generally cooperative.

Q 1.3.6 Please describe a typical case or scenario.

(2) Preservation of traffic data
In investigating an illegal access (e.g. a perpetrator played internet games using a forged ID), authorities have preserved traffic data (log) concerning the perpatrator's access to the internet through an ISP which administers the relevant IP address.

(3) Preservation (seizure) of computer data other than traffic data
In investigating a case concerning a computer virus saved on a web server, authorities identified the URL of the server on which the virus was saved, and seized the computer data stored in the said server upon showing a seizure warrant issued by a judge to the administrator of the server.

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

Preservation request of traffic data (Art. 197(3) of the Code of Criminal Procedure) is considered an effective, simple and prompt tool for an investigation as it can be executed without a warrant issued by a judge. However, a preservation request is only effective when an ISP retains the data that are being sought. When an ISP does not retain those data in the first place or when the data retention period is extremely short, authorities are unable to obtain the necessary data even if authorities have sent a preservation request.

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

2.1 Legislation/regulations

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

Art. 218 and Art. 197(3) of the Code of Criminal Procedure (please refer to Q1.1.1).

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

Authorities exchange information with some service providers to facilitate seizure process; for instance they exchange information on the location to execute a seizure warrant and how to describe the "object to be seized" in a seizure warrant (e.g. the name of service and account should be clearly described, Universal Time Coordinated (UTC) should be used to describe the period for disclosure, etc).

2.2 Procedures

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

The procedure for preservation and seizure of traffic data is as follows:

(1) Investigating authorities specify the traffic data (IP address, access date and time) necessary for investigation and the administrator of such IP address.
(2) Public prosecutor, public prosecutor's assistant officer or a judicial police official (hereinafter referred to as "investigating officials") drafts the preservation request document and sends it to the administrator such as a service provider.
(3) Investigating officials request for issuance of a seizure warrant to a judge and receives the warrant.
(4) Investigating officials show the seizure warrant to the administrator (a service provider) and seize the data specified in the warrant upon submission by the administrator (service providers).

2.3 Practical experience

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

Art. 197 of the Code of Criminal Procedure does not provide for a partial disclosure, and we provide a full disclosure of data promptly through a seizure pursuant to Art. 218 of the Code of Criminal Procedure. Service providers do not submit traffic or other data voluntarily to the authorities with a view to protecting secrecy of communication and personal information. The authorities can only obtain traffic or other data upon issuance of a seizure warrant by a judge.

Q 2.3.2 How frequently do you use these provisions?

See Q 1.3.2.

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

The time required to seize traffic data from the moment of preservation of such data differs among service provider. While there are no detailed statistics, the authorities presume that it generally takes 2 weeks to 1 month.

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

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

3.1 Legislation/regulations

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

- Art. 3, Art. 5, Art. 8(1)vi and Art. 8(2) of the Act on International Assistance in Investigation and Other Related Matters
- Art. 197(3) of the Code of Criminal Procedure (please refer to Q1.1.1.)

The Act on International Assistance in Investigation and Other Related Matters

Art. 3

(1) A request for assistance shall be received, and evidence shall be forwarded to the requesting country, by the Minister of Foreign Affairs; except that the Minister of Justice shall carry out these tasks when a treaty confers the authority to receive requests for assistance on the Minister of Justice or when the Minister of Foreign Affairs gives consent in an emergency or under other special circumstances.

(2) When the Minister of Justice receives a request for assistance or forwards evidence to the requesting country pursuant to the proviso of the preceding paragraph, the Minister of Justice may ask the Minister of Foreign Affairs for cooperation necessary for the execution of matters relating to the assistance.

Art. 5

(1) With respect to a request for assistance in matters other than a transfer of a sentenced inmate for testimony, except where any item in Article 2 (any item in Article 2 or 4 when the Minister of Justice receives a request for assistance pursuant to the proviso of paragraph (1) of Article 3) applies, the Minister of Justice shall, when none of the provisions of the following paragraph applies and the Minister of Justice deems it appropriate to honor the request, take one of the following measures:

(i) Send the related documents to the Chief Prosecutor of an appropriate district public prosecutors office and order the Chief Prosecutor to collect the evidence necessary for assistance;

(ii) Send the documents concerning the request for assistance to the National Public Safety Commission;

(iii) Send the documents concerning the request for assistance to the Commandant of the Japan Coast Guard, or to the head of other national agencies to which judicial police officials belong as provided by Article 190 of the Code of Criminal Procedure (Act No. 131 of 1948).

(2) With respect to a request for provision of a document pertaining to the trial which is in the custody of a court, a public prosecutor or a judicial police officer, the Minister of Justice shall send the documents pertaining to the request for assistance to the custodian of the document pertaining to the trial.

(3) The Minister of Justice may conduct an inquiry on the whereabouts of any relevant person and other necessary matters, when the Minister of Justice deems it necessary in order to take the measures provided in paragraph (1) or any other measures relating to the assistance.

Art. 8

(1) [*Translation is not available for this paragraph. In summary, Art. 8(1)vi provides that, in order to collect evidence necessary for mutual legal assistance, a public prosecutor or a judicial police official may request in writing the service providers or persons/entities with local network facility not to delete the necessary traffic data for no more than 30 days (or if extension is requested, for no more than 60 days).]*

(2) With regard to the collection of evidence necessary for assistance, a public prosecutor or a judicial police officer may, if it is deemed to be necessary, undertake seizure, search, or inspection of evidence, upon a warrant issued by a judge.

[…]

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

(1) Competence for receiving request

- The Minister of Justice for the international preservation requests pursuant to bilateral/multilateral mutual legal assistance treaties/agreements and the Cybercrime Convention
- The Minister for Foreign Affairs for all the other preservation requests if made as a mutual legal assistance request (and the Minister for Foreign Affairs transfers the request to the Minister of Justice)
- The National Public Safety Commission (the National Police Agency) for a request through 24/7 Network based on the Cybercrime Convention, the G8 24/7 network and ICPO channel.

(2) Competence for executing a request

Public prosecutor or judicial police official executes the request.

(When the Ministry of Justice receives an international preservation request, either of the following two procedures is followed (Art. 8(1) and Art. 8(2) of the Act on International Assistance in Investigation and Other Related Matters):

(1) The Minister of Justice receives the request and orders a Chief Prosecutor of an appropriate district public prosecutors' office to execute the request. Chief Prosecutor then have a public prosecutor in the office execute the request.

(2) The Minister of Justice receives the request and sends the documents concerning the request for assistance to the National Public Safety Commission (the National Police Agency), which then instructs the appropriate Prefectural Police to execute the request. The Superintendent General or the chief of the Prefectural Police then have a judicial police officer of the Prefectural Police execute the request.)

(3) The role of the contact point and ICPO channel

The 24/7 point of contact based on the Cybercrime Convention or ICPO channel is the International Investigative Operations Division of the National Police Agency. When it receives a preservation request from foreign authorities based on the Cybercrime Convention or through ICPO channel, the Division instructs the appropriate Prefectural Police to execute the request.

On the other hand, the 24/7 point of contact for the G8 24/7 network is the Cybercrime Division of the National Police Agency. Therefore, a preservation request from foreign authorities through G8 24/7 network is received by the Cybercrime Division. G8 24/7 network has been effective in promptly preserving traffic data. Similar to the request based on the Convention, preservation request through G8 24/7 network is also executed by the appropriate Prefectural Police.

Q 3 1 3 What rules apply for the transfer of the data preserved to foreign authorities?

There needs to be a request from a foreign authority to transfer the said data. Pursuant to Art. 14(5) of the Act on International Assistance in Investigation and Other Related Matters, the Minister of Justice may, where necessary, determine conditions that the requesting country must observe with respect to the use or return of the evidence.

The Act on International Assistance in Investigation and Other Related Matters

Art. 14

(1) When the Chief Prosecutor has completed the collection of evidence necessary for the assistance, he/she shall promptly send the collected evidence with his/her opinion attached, to the Minister of Justice. When the head of a national agency set forth in paragraph (1), item (iii) of Article 5 has completed the collection of evidence, the same shall apply.

(2) When a Chief of Police has completed the collection of evidence necessary for the assistance, the Prefectural Public Safety Commission shall promptly send the collected evidence with its opinion attached, to the National Public Safety Commission.

(3) Upon receiving the evidence pursuant to the provision set forth in the preceding paragraph, the National Public Safety Commission shall promptly send the evidence with its opinion attached, to the Minister of Justice.

(4) The custodian of a document relating to the trial who has received the documents concerning a request for assistance pursuant to the provision of paragraph (2) of Article 5, shall promptly send the document or a certified transcript thereof with his/her opinion attached, to the Minister of Justice; but when he/she is unable to do so, he/she shall return the documents concerning the request for assistance to the Minister of Justice.

(5) When, after receiving the evidence set forth in paragraph (1),(3), or the preceding paragraph, the Minister of Justice deems it to be necessary, he/she shall determine conditions that the requesting country shall observe with respect to the use or return of the evidence.

(6) When the requesting country does not assure that it will observe the conditions set forth in the preceding paragraph, the Minister of Justice shall not provide the assistance.

3.2 Procedures

Q 3.21 Please describe the end-to-end procedure for the handling of the request.

(1) The Minister of Justice receives requests pursuant to bilateral/multilateral MLA treaties/agreements and the Cybercrime Convention. With respect to all the other requests, the Minister for Foreign Affairs receives the requests and sends them to the Minister of Justice. (The requests sent through ICPO are received directly by the National Police Agency.)

(2) The Minister of Justice checks if the request satisfies the conditions stipulated by a domestic implementing legislation such as whether the request is not for a political offense. When the request is deemed to satisfy the conditions, the Minister of Justice either (a) orders a Chief Prosecutor of an appropriate district public prosecutors' office to execute the request, or (b) sends the documents concerning the request for assistance to the National Public Safety Commission (the National Police Agency).
(3) In case of (a): Chief Prosecutor of a district public prosecutors' office have a public prosecutor in the office execute the request and reports the outcome to the Minister of Justice.
(4) In case of (b): The National Public Safety Commission the National Police Agency) identifies the traffic data (IP address, access date and time) and the administrator of IP address specified in the preservation request document. It then instructs the Prefectural Police overseeing the location of the said administrator to execute the request. The Prefectural Police requests the administrator of the IP address to preserve the data concerned and report the outcome to the National Public Safety Commission (the National Police Agency). The National Public Safety Commission (the National Police Agency) then sends the outcome to the Minister of Justice.
(5) With respect to requests made pursuant to bilateral/multilateral MLA treaties/agreements and the Cybercrime Convention, the Minister of Justice directly replies to the requesting state. With respect to all the other MLA requests, the Minister for Foreign Affairs replies to the requesting state. (With respect to requests sent through ICPO, the National Police Agency replies directly to the requesting state).

Furthermore, the procedure to receive and execute the international preservation request sent through G8 24/7 network is as follows;

(1) The National Police Agency receives the preservation requests and determines the administrator of the traffic data (IP address, access date and time) and IP address specified in the preservation request document.
(2) The National Police Agency then instructs the Prefectural Police overseeing the location of the said administrator to execute the request.
(3) The Prefectural Police requests the administrator of the IP address to preserve the data concerned and report the outcome to the National Police Agency.
(4) The National Police Agency then communicates the outcome directly to the requesting foreign authorities.

Q 3 .2.2 What templates/forms are used for international requests? Please attach if any.

We do not use any templates or forms.

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

There is no additional information necessary. However, please note that the information on the access date and time for the IP address must be specified by second.

3.3 Practical experience

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

(1) Mutual Legal Assistance Treaty/Agreement or diplomatic channel

In 2013, Japan has neither sent nor received any international preservation request through the Cybercrime Convention 24/7 contact points, MLA Treaty/Agreement central authorities or diplomatic channel.

(2) ICPO channel (police-to-police cooperation)
In 2013, Japan has not received any foreign preservation request through ICPO, but has sent 124 preservation requests to foreign authorities through ICPO.

(3) G8 24/7 network channel
In 2013, Japan has received 5 foreign preservation requests through G8 24/7 network and has sent 40 preservation requests to foreign authorities through G8 24/7 network.

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

When we receive preservation request through G8 24/7 network, we issue the request to the service provider in 1 day at the earliest and within 1 week at most.

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

- With respect to preservation request through ICPO channel, the average time for notification is approximately 11 days from the date we send the request to foreign authority.
- With respect to preservation request through G8 24/7 network, we are notified in 1 day at the earliest and within approximately 1 month at most from the date we send the request to foreign authority.

Q 3.3.4 Please describe a typical case or scenario.

(1) As a requesting state
In a case concerning illegal access, the investigation found out that the ISP administering the relevant IP address is located abroad. Our authorities therefore sent the request for preservation of traffic data to the authorities abroad. In sending the preservation request, we have specified that we will follow up by MLA request to obtain the said traffic data.

(2) As a requested state
In a case concerning mass e-mails containing URL of a web server in which computer virus are stored, the foreign investigation found out that the relevant IP address is located in Japan. We have therefore received the request for preservation of traffic data from the foreign authorities. The preservation request specified that the authorities will follow up by MLA request to obtain the said traffic data.

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

In cybercrime investigation, it is extremely important to obtain traffic data as it leads to identification of the suspect. However, traffic data can be deleted within a short period while, in general, it takes considerable amount of time to obtain evidence through MLA process. Therefore, without provisions on preservation, it may become very difficult to obtain traffic data.

Q 3 3 6 How often are international preservation requests that you receive not followed by mutual legal assistance requests?

In 2013, Japan received 5 foreign preservation requests through G8 24/7 network and, among them, executed 4 requests for which the data had been retained. For the 2 requests among the 4 requests, we have not received the follow-up MLA request (as of the end of July, 2014).

Q 3.3 7How often do you send international preservation requests and not follow them with mutual legal assistance requests or notifications?

(1) Request made through ICPO

In 2013, Japan sent 124 preservation requests to foreign authorities through ICPO channel. For 5 cases among them, we have been notified that the preservation request has been issued. For 2 cases among the above 5 cases, we have sent the follow-up MLA request, while for the rest of the 3 cases, we have neither sent the follow-up MLA request nor notified the foreign authorities that there will be no further MLA request.

(2) Request made through G8 24/7 network

In 2013, Japan sent 40 preservation requests to foreign authorities through G8 24/7 network. Out of the 40 requests, we have sent the follow-up MLA request to transfer the preserved data with respect to 33 cases, while for the rest of 7 cases, we did not send any follow-up MLA request. Generally, we notify the foreign authorities if there will be no further MLA request.

Q 3 3 8In conclusion: What are the main strengths and what are the main problems of preservation within the framework of international cooperation?

(1) Strengths

Japan can implement international requests for preservation of traffic data through all the channels, such as G8 24/7 network, ICPO, contact points for the Cybercrime Convention, central authorities of bilateral/multilateral MLA Treaties/Agreements and diplomatic channel. [Seizure of computer data can be implemented in response to requests received through central authorities of MLA treaties and diplomatic channels.]

(2) Problems

Since Japan does not have a data retention system, there are times where the traffic data for which preservation is requested are already erased at the service provider.

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

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

4.1 Legislation/regulations

Q 4 1 1 What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

Art. 3, Art. 5, Art. 8(1)vi, Art. 8(2) and Art. 14 of the Act on International Assistance in Investigation and Other Related Matters (please refer to Q3.1.1 for Art. 3, 5 and 8; please refer to Q3.1.3 for Art. 14)

Q 4 12 What are the conditions, limitations or impediments to disclosing a sufficient amount of traffic data?

Pursuant to Art. 14(5) of the Act on International Assistance in Investigation and Other Related Matters, the Minister of Justice may, where necessary, determine conditions that the requesting country must observe with respect to the use or return of the evidence.

4.2 Procedures

Q 4.2 1 Please describe the end-to-end procedure for the handling of a request.

(1) The Minister of Justice receives the requests pursuant to bilateral/multilateral MLA treaties/agreements and the Cybercrime Convention. With respect to all the other requests, the Minister for Foreign Affairs receives the requests and sends them to the Minister of Justice.
(2) The Minister of Justice checks if the request satisfies the conditions stipulated by a domestic implementing legislation such as whether the request is not for a political offense. When the request is deemed to satisfy these conditions, the Minister of Justice either (a) orders a Chief Prosecutor of an appropriate district public prosecutors' office to collect the evidence, or (b) sends the documents concerning the request for assistance to the National Public Safety Commission (the National Police Agency).
(3) In case of (a): Chief Prosecutor of the district public prosecutors' office have a public prosecutor in the office collect the evidence necessary for the assistance and sends the evidence collected to the Minister of Justice.
(4) In case of (b): The National Public Safety Commission (the National Police Agency) determines the traffic data (IP address, access date and time) and the administrator of IP address specified in the preservation request document. It then instructs the Prefectural Police overseeing the location of the said administrator to collect the evidence necessary for assistance. The Superintendent General or the chief of the Prefectural Police then have a judicial police officer of the Prefectural Police collect the evidence. The Prefectural Police sends the evidence to the National Public Safety Commission (the National Police Agency). The National Public Safety Commission (the National Police Agency) then sends the evidence to the Minister of Justice.
(5) With respect to requests made pursuant to bilateral/multilateral MLA treaties/agreements and the Cybercrime Convention, the Minister of Justice sends the evidence directly to the requesting state. With respect to all the other MLA requests, the Minister for Justice sends the evidence to the Minister of Foreign Affairs who then will send the evidence to the requesting state.

4.3 Practical experience

Q 4.3.1 How frequently do you use this provision?

In 2013, the National Police Agency seized traffic data for 3 cases pursuant to Art. 8(2) of the Act on International Assistance in Investigation and Other Related Matters.

Q 4.3.2 Please describe a typical case or scenario.

In a case concerning mass e-mails containing URL of a web server in which computer virus are stored, the foreign investigation found out that the relevant IP address is located in Japan. We have therefore received the request for preservation of traffic data from the foreign authorities and implemented the request.

The preservation request was then followed up by the MLA request to obtain the said traffic data. The court issued a seizure warrant and the authorities sent the seized traffic data to the requesting authority.

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

Japan implements "expedited disclosure of preserved traffic data" as defined in Art. 30 of the Cybercrime Convention by promptly seizing the preserved traffic data based on Art. 8(2) of the Act on International Assistance in Investigation and Other Related Matters. Up until now, there has been no problem.

6.9 Mauritius

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).

Mauritius has, through the Computer Misuse and Cybercrime Act 2003, made legal provisions for the expedited preservation of stored data . Section 11 of the Act (reproduced below) stipulates that an investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data.

*11. **Preservation order***
*(1) Any investigatory authority may apply to the Judge in Chambers for an order for the **expeditious preservation of data** that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.*
*(2) For the purposes of subsection (1), data includes **traffic data and subscriber information**.*
(3) An order made under subsection (1) shall remain in force—
(a) until such time as may reasonably be required for the investigation of an offence;
(b) where prosecution is instituted, until the final determination of the case; or
(c) until such time as the Judge in Chambers deems fit.

The term investigatory authority has been defined in the Act as "*the police or any other body lawfully empowered to investigate any offence".*

Q 1 1 2 Do they cover all types of data (traffic, content) stipulated by article 16?

The preservation order may include all types of data. Section 11 (2) of the Computer Misuse and Cybercrime Act 2003 (as reproduced above) stipulates that data **includes traffic data and subscriber information.**

It is also important to note that data has been given a broad definition under the Act. In its interpretation section *"data" is defined as follows –*
"data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose, and includes representations of facts, information and concepts held in any removable storage medium.

Q 1 1 3 Do they apply to electronic evidence in relation to any criminal offence or are there limitations? Please explain.

The preservation order applies to electronic evidence in relation to any criminal offence.
Under section 11 of the Computer Misuse and Cybercrime Act 2003 (as reproduced above) any investigating authority may apply to the Judge in Chambers for the issue of a preservation order of data stored by means of a computer system or any other information and communication technologies.

Moreover section 11 (3)(a) makes reference to " *…investigation of an* ***offence****..",* which includes any offence and section 11(3)(b) makes reference to "*…where* ***prosecution*** *is instituted…*" which includes prosecution of 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 no such agreements and most data are obtained through Judge's Order.

Q 1 1 5 Is preservation visible to the suspects or account holder or can you prevent disclosure of the preservation request?

The preservation order can be made ex parte, that is without it being served on the suspect and may be issued without his knowledge. However, the Judge will require that the request be served on the suspect for him to show cause why the order should not be discharged. Thus, although the suspect may be unaware of the preservation request initially, once it is issued against the suspect the latter will become aware of the preservation request.

1.2Procedures Q 1.2.1 Please describe the end-to-end procedure for the handling of a request.

As stated earlier preservation orders are very rarely sought.

Q 1. 2. 2 What templates/forms are used? Please attach if any.

There is no template

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?

In practice, preservation orders are rarely sought. Investigative authorities rely more on sections 13 and 14 of the Computer Misuse and Cybercrime Act 2003. Section 13 provides for production orders while section 14 of the Act provides for powers of access, search and seizure for purposes of investigation.

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

Very rarely

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?

Preservation has been foreseen in our procedural law .Preservation Order under section 11 of the Computer Misuse and Cybercrime Act 2003 (as reproduced above) stands on its own that is, authorities do not need to obtain preservation through search, production orders or other powers.

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

Preservation requests are very rarely served on physical or legal persons.

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

As stated earlier preservation requests are very rarely relied on.

Q 1.3.6 Please describe a typical case or scenario.

As stated earlier preservation requests are very rarely relied on.

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 preservation systems is that we have statutory provisions, section 11 of the Computer Misuse and Cybercrime Act (as reproduced above), that has already been enacted to obtain the expeditious preservation of computer data, including traffic data.

The main problems in relation to our preservation system cannot be assessed at this stage because, as stated above, our investigatory authorities very rarely apply for Preservation Orders.

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

2.1 Legislation/regulations

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

The relevant provisions of the law are sections 12 and 13 of the Computer Misuse and Cybercrime Act 2003 as reproduced below.

12. ***Disclosure of preserved data***

The investigatory authority may, for the purposes of a criminal investigation or the prosecution of an offence, apply to the Judge in Chambers for an order for the ***disclosure*** *of—*

(a) all ***preserved data****, irrespective of whether one or more service providers were involved in the transmission of such data;*

(b) sufficient data to identify the service providers and the path through which the data was transmitted; or

(c) electronic key enabling access to or the interpretation of data.

13. Production order

(1) Where the ***disclosure*** *of data is required for the purposes of a criminal investigation or the prosecution of an offence, an investigatory authority may apply to the Judge in Chambers for an order compelling—*

(a) any person to submit specified data in that person's possession or control, which is stored in a computer system; and

(b) any service provider offering its services to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material to which an investigation relates consists of data stored in a computer, disc, cassette, or on microfilm, or preserved by any mechanical or electronic device, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is visible and legible.

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

There are no such agreements. Investigating authorities rely more on Judges Orders for disclosures of information.

2.3 Practical experience

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

Complaints are made to the Police. During enquiry, the Police liaises with the Office of the Director of Public Prosecutions if traffic data is required. The office of the Director of Public Prosecutions then initiates all legal proceedings, mainly through Judges Order, to obtain the information.

2.3 Practical experience

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

It is very important.

Q2.3.2 How frequently do you use these provisions?

Very often.

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

Generally Judges Orders are obtained within 15 days but it may take up to 6 month to obtain the traffic data.

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

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

3.1 Legislation/regulations

Q3 1 1 What legal provisions/regulations do you apply for executing an international request for preservation? Please list and attach text.

- There is no specific provision under the Mutual Assistance in Criminal and Related Matters Act which governs the execution of an international request for preservation of stored computer data. However, where there is a request by a foreign State, or an international criminal tribunal to obtain a search warrant for the search of a property, and removal or seizure of any document or article (eg a computer and related equipment), an application may be made by the Central Authority of Mauritius under the Act for the issue of a search warrant and for seizure.

Although section 11 of the Computer Misuse and Cybercrime Act provides under section 11 that a*ny investigatory authority may apply to the Judge in Chambers for an order for the* ***expeditious preservation of data*** *that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification,* it would seem that one **cannot rely on this provision to provide data to a foreign State** in view of the fact that it is only an investigatory authority which may make an application for such an order to the Judge in Chambers. This is due to the fact that the Act defines investigatory authority as the police or any other body lawfully empowered to investigate any offence. Unfortunately, the definition as it presently stands does not allow international requests to be entertained unless there is an offence which is also committed in Mauritius which would involve a joint investigation by both the foreign authority and local investigatory authority.

Q3.1.2 Who has the competence for receiving and executing the international preservation request? What is the role of the contact point?

As stated above there is no specific provision under the Mutual Assistance in Criminal and Related Matters Act and as per records no such requests have been received up to now. However under section 5 of the Mutual Assistance in Criminal and Related Matter Act, a foreign State may, in relation to a serious offence, and an international criminal tribunal may, in relation to an international criminal tribunal offence, make a request for assistance to the Central Authority in any proceedings commenced in the foreign State or before the international criminal tribunal, as the case may be. The Central Authority in the Act means the Attorney General.

Q3.1.3 What rules apply for the transfer of the data preserved to foreign authorities?

There are no specific provisions for the transfer of the data preserved to foreign authorities under the Mutual Assistance in Criminal and Related Matters Act. However section 6 of the Act (as reproduced below) provides that when the Central Authority grants a request by a foreign State, or an international criminal tribunal, to obtain evidence or a search warrant in Mauritius, the Central Authority may apply to a Judge in Chambers for an evidence gathering order or a search warrant for the search of a person or premises, and removal or seizure of any document or article.

*6. **Procedure** for an **evidence-gathering order** or a **search warrant***

(1) Notwithstanding any other enactment, where the Central Authority grants a request by a foreign State, or an international criminal tribunal, to obtain evidence or a search warrant in Mauritius, the Central Authority may apply to a Judge in Chambers for—

(a) an evidence-gathering order; or

(b) a search warrant for the search of a person or premises, and removal or seizure of any document or article.

(2) Subject to section 5 (5), a request by a foreign State, or an international criminal tribunal, for an evidence-gathering order shall—

(a) comply with the requirements in section 4 (3);

(b) specify—

(i) the name and address or the official designation of the person to be examined;

(ii) the question to be put to the person or the subject matter about which he is to be examined;

(iii) whether it is desired that the person be examined orally or in writing;

(iv) whether it is desired that an oath be administered to the person;

(v) any provision of the law of the foreign State as to privilege or exemption from giving evidence which appears especially relevant to the request;

(vi) any special requirements of the law of the foreign State as to the manner of taking evidence relevant to its admissibility in that State;

(vii) the document, record or property to be inspected, preserved, photographed, copied or transmitted;

(viii) the property of which samples are to be taken, examined or transmitted; and

(ix) the site to be viewed or photographed.

(3) A request by a foreign State or an international criminal tribunal for a search warrant shall—

(a) comply with the requirements in section 4 (3);

(b) specify the property to be searched for and seized; and

(c) contain such information available to the foreign State or international criminal tribunal, as the case may be, as may be required for the purpose of the application.

(4) (a) Subject to subsection (9), the Judge in Chambers shall grant an application for an evidence-gathering order where he is satisfied that there are reasonable grounds to believe that—

(i) a serious offence has been or may have been committed against the law of the foreign State or an international criminal tribunal offence has been or may have been committed; and

(ii) evidence relating to an offence referred to in subparagraph (i) may be—

(A) found in Mauritius; or

(B) given or produced by a person believed to be in Mauritius.

(b) The Judge in Chambers shall not grant an application for a search warrant where it would, in all the circumstances, be more appropriate to grant an evidence-gathering order.

(5) For the purposes of subsection (4) (a) (i), a statement contained in the request to the effect that—

(a) a serious offence has been or may have been committed against a law of the foreign State; or

(b) an international criminal tribunal offence has been or may have been committed,

shall be prima facie evidence of that fact.

(6) An evidence-gathering order—

(a) shall provide for the manner in which the evidence is to be obtained in order to give effect to the request and may require any person named therein to—

(i) make a record from data or make a copy of a record;

(ii) attend before the Master and Registrar to give evidence; and

(iii) produce to the Judge in Chambers, or to any other person designated by him, any article, including any document, or copy thereof; or

(b) may include such terms and conditions as the Judge in Chambers considers desirable, including those relating to—

(i) the interests of the person named therein or of third parties; or

(ii) the questioning of the person named therein by any representative of the foreign State or international tribunal, as the case may be.

(7) Subject to subsections (8) and (9), a person named in an evidence-gathering order may refuse to answer a question, or to produce a document or article, where the refusal is based on—

(a) an enactment which permits the person to decline to give evidence in similar circumstances in proceedings originating in Mauritius or a privilege recognised by the law in Mauritius;

(b) a privilege recognised by a law in force in the foreign State that made the request; or

(c) a law currently in force in the foreign State that would render the answering of that question, or the production of that document or article by that person, in his own jurisdiction, an offence.

(8) (a) Where a person refuses to answer a question or to produce a document or article pursuant to subsection (7) (b) or (c), the Central Authority shall notify the foreign State and request the foreign State to provide a written statement on whether the person's refusal was well founded under the law of the foreign State.

(b) A written statement received by the Central Authority from the foreign State in response to a request under paragraph (a) shall be admissible before the Judge in Chambers and, for the purposes of this section, be conclusive evidence that the person's refusal is, or is not, well founded under the law of that State.

(c) Any person who, without reasonable excuse, refuses to comply with an order of a Judge in Chambers made under this section or who, having refused to answer a question or to produce a document or article on a ground specified in subsection (7), continues to refuse notwithstanding the admission into evidence of a statement under paragraph (b) to the effect that the refusal is not well founded, shall be in contempt of Court.

(9) Notwithstanding section 26 of the Bank of Mauritius Act, section 64 of the Banking Act , section 83 of the Financial Services Act and subsections (7) and (8), a Judge in Chambers hearing a request from a foreign State or an international criminal tribunal may grant an evidence-gathering order or search warrant against the Bank of Mauritius, a bank or financial institution where he is satisfied that—

(a) the information is material and necessary to the proceedings in the foreign State or before the international criminal tribunal; and

(b) the law of the foreign State permits the disclosure of information to foreign States in circumstances similar to the one relating to the request.

(10) The Central Authority shall inform the foreign State of the date and place of the taking of evidence pursuant to this section.

(11) The Judge in Chambers may authorise the presence of representatives of the foreign State, and of parties to the relevant proceedings in the foreign State, at the proceedings under this section.

(12) The Central Authority shall provide such authenticated report as may be required by the foreign State, or international criminal tribunal, concerning—

(a) the result of any search;

(b) the place and circumstances of seizure; and

(c) the subsequent custody of the property seized.

3.2.Procedures

Q3.2.1.Please describe the end-to-end procedure for the handling of the request.

There is no end-to-end procedure for handling requests for transfer of the data preserved to foreign authorities. However general handling of international requests in criminal matters are dealt by the Attorney General who acts as the Central Authority as stipulated under the Mutual Assistance in Criminal and Related Matters Act. The Attorney General executes the requests as stipulated by section 5 (3) of the Act,"…… *The Central Authority may, in respect of a request under subsection (1) from an international criminal tribunal, grant the request, in whole or in part, on such terms and conditions as it thinks fit*."

Q3.2.2 What templates/forms are used for international requests? Please attach if any.

There is no template/forms used for international requests.

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

There are no specific provisions for the transfer of the data preserved to foreign authorities under the Mutual Assistance in Criminal and Related Matters Act.

3.3 Practical experience

Q3.3.1 How frequently do you send and receive international preservation requests? Please provide estimated numbers if readily available.

Mauritius has never sent international preservation orders; we have not received any preservation order request up to now.

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

This question is not applicable in Mauritius since as stated above there are no specific provisions for the transfer of the data preserved to foreign authorities under the Mutual Assistance in Criminal and Related Matters Act. However for other requests generally they may be entertained and responded to within a delay of up to approximately 3 months, depending on the nature of the request.

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

Mauritius has never asked for expedited preservation of stored computer data to foreign countries.

Q 3.3.4 Please describe a typical case or scenario.

As stated earlier Mauritius has never asked for preservation of stored computer data to foreign countries.

Q3.3.5 Without provisions on preservation, would this create problems for international cooperation?

Our law will have to be amended to address this issue which is considered to be crucial in tackling cybercrime.

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

None because of our legal provisions as stated above under Q3.1.1

Q3.3.7 How often do you send international preservation requests and not follow them with mutual legal assistance requests or notifications?

Mauritius has never sent any foreign preservation requests.

Q3.3.8 In conclusion: What are the main strengths and what are the main problems of preservation within the framework of international cooperation?

The strength is that in our system we already have the possibility to obtain preservation orders. The weakness is that our law does not cater for the possibility of entertaining such requests as explained under Q 3.1.1. We propose to amend our legislation to cure this lacuna.

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

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

4.1.Legislation/regulations

Q 4 1 1 What legal provisions/regulations allow you to disclose a sufficient amount of traffic data (as defined in Article 30.1) to foreign authorities? Please list and attach text.

There are no legal provisions/regulations that allows Mauritius to disclose sufficient amount of traffic data. Section 17 of the Computer Misuse and Cybercrime Act, as reproduced below, deals with disclosure of data and information. It must be noted that under sections 11 to 15 of the Act only an investigatory authority can make appropriate requests the Judge in Chambers; investigatory authority under the Act has been given a narrow definition and does not include foreign authorities.

It must be noted that requests for international disclosures of data can be acceded to only where there is an offence which is also committed in Mauritius which would involve a joint investigation by both a foreign authority and a local investigatory authority. This has been explained above under Q3.1.1.

17. Limited use of disclosed data and information
No data obtained under sections 11 to 15 shall be used for any purpose other than that for which the data was originally sought except—

(a) in accordance with any other enactment;

(b) in compliance with an order of a Court or Judge;

(c) where such data is required for the purpose of preventing, detecting or investigating offences, apprehending or prosecuting offenders, assessing or collecting tax, duty or other monies owed or payable to the Government;

(d) for the prevention of injury or other damage to the health of a person or serious loss of or damage to property; or

(e) in the public interest.

Q 41.2.What are the conditions, limitations or impediments to disclosing a sufficient amount of traffic data?

The main limitation is that international disclosure can only take place when there is joint investigation involving local and international investigatory authorities as explained in detailed under Q3.1.1.1.

4.2.Procedures

Q4.2.1Please describe the end-to-end procedure for the handling of a request.

There is no end-to-end procedure for handling requests for disclosure of sufficient amount of traffic data. However as stated under Q3.2.1 general handling of international requests in criminal matters are dealt with by the Attorney General.

4.3.Practical experience

Q4.3.1.How frequently do you use this provision?

Mauritius has never made use of this provision as explained under Q 4.2.1.1

Q 4.3.2.Please describe a typical case or scenario.

This question is not relevant for reasons given above.

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

Provisions on partial disclosure are needed and without same problems of international cooperation are bound to occur.