Electronic Evidence Country Fiche: SRI LANKA

1) DEFINITIONS

Sri Lanka
What are the definitions in your laws/regulations, if any, of:
Electronic evidence
In the legislation of Sri Lanka, the term "electronic evidence" is not explicitly defined but *"*electronic record" is included in Section 38, Interpretation, Part III Miscellaneous, of the Computer Crime Act, 2007 and it means, information, record or data generated, stored, received or sent in an electronic form or microfilm, or by any other similar means. "Electronic record" is also included in Section 26, Interpretation, Chapter VI Miscellaneous, of the Electronic Transactions Act No.19, 2006 which refers to a written document, or other record created, stored, generated, received, or communicated by electronic means. Additionally, within the same Section 26 the term "electronic" means information generated, sent received or stored by electronic, magnetic, optical, or similar capacities regardless of the medium. Based on the same provision: *"*electronic document*"* includes documents, records, information, communications or transactions in electronic form.
Computer system
The term "computer system" is explicitly defined as "a computer or group of interconnected computers, including the internet" under Section 38, Interpretation, Part III Miscellaneous, of the Computer Crime Act, 2007. Moreover, referring to the source of electronic data, the same article includes the definition of "computer" as "an electronic or similar device having information processing capabilities".
Computer data
Sri Lankan legislation does not explicitly provide definition for the term "computer data". However, the term "data message" is described under Section 26, Interpretation, Chapter VI Miscellaneous, of the Electronic Transactions Act No.19, 2006 as "information generated, sent, received or stored by electronic, magnetic, optical or other similar means".

Categories of computer data (e.g. basic subscriber information, traffic data and content data)
Sri Lankan legislation does not explicitly provide definition for each specific type of data. However, the term "Subscriber data" is defined under the qualification of "Subscriber information" in Section 38, Interpretation, Part III Miscellaneous, of the Computer Crime Act, 2007 as "any information, contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services". The same definition can be found in Section 26 Interpretation, Chapter VI Miscellaneous, of the Electronic Transactions Act No.19, 2006. The term "traffic data" is included in Section 38, Interpretation, Part III Miscellaneous, of the Computer Crime Act 2007. "Traffic data" means data— (a) that relates to the attributes of a communication by means of a computer system; (b) data generated by a computer system that is part of a service provider; and (c) which shows communications origin, destination, route, time, data, size, duration or details of subscriber information. The term "Content data" appears not to be defined. Additionally, in Sri Lanka, there is a specific format issued in the Schedule of the Mutual Assistance in Criminal Matters law (MACM) when requesting information from the Central Authority of Sri Lanka. Under item 4.1 of the standard form, there is an option reserved for requesting assistance to obtain the expedited preservation of computer data or traffic data. The said format is available at https://www.moj.gov.lk/images/pdf/other/Form24-2018_E.pdf.
Electronic surveillance or real-time collection of computer/communication data
Within the legal framework of Sri Lanka, neither a specific definition of "real-time collection" nor the term "Electronic surveillance" appear to be explicitly provided. However, the Computer Crimes Act, No. 24 of 2007 Powers of search and seizure with warrant Section 18, includes interception of communications and traffic data real-time. It provides for power of the police for the purpose of investigation as follows: (i) obtain any information including subscriber information and traffic data in the possession of any service provider; (ii) intercept any wire or electronic communication including subscriber information and traffic data, at any stage of such communication […]
Service provider (e.g. ISP, hosting)
According to Section 38, Interpretation, Part III Miscellaneous, of the Computer Crime Act, 2007 the term "service provider" refers to— (a) a public or private entity which provides the ability for its customers to communicate by means of a computer system; and (b) any other entity that processes or stores computer data or information on behalf of that entity or its customers.

UNODC
United Nations Office on Drugs and Crime

2) DATA RETENTION REGIME

Sri Lanka
Do you have any domestic laws that stipulate a mandatory retention period of electronic data? If so, for what types of data and for how long?
The Electronic Act, 2006, Chapter II, Recognition Data Message and Other Communications in Electronic Form sets the general requirement for retentions. Under Section 6, the requirement under any law that information be retained, shall be deemed to be satisfied by the retention in electronic form of information contained in a data message, electronic document, electronic record or other communication notwithstanding the fact that such information was not originally generated in electronic form, if— (a) the information in the data message, electronic document, electronic record or communication is accessible so as to be usable for subsequent reference; and (b) the data message, electronic document, electronic record or communication is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and (c) such information, enables the identification of the origin and destination of the data message, electronic document, electronic record or other communication and the date and time when such information was generated, sent or received, is retained. Provided that the provisions of this section shall not apply to any information, which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received. Additionally, the Data Protection Act, 2022 establishes the obligation to limit the period of retention only for such period as may be necessary or required for the purposes for which such personal data is processed. Despite the above provision in Sri Lanka, there are no general retention requirements. A specific timeframe is indicated only for the following specific sectors: - The Financial Transactions Reporting Act, Section 4, mandates retention period of 6 years, unless the Financial Intelligence Unit requests retention for a longer period. - The Right to Information Act (RTI Act) mandates that public authorities maintain all its records for a period of 10 years for data generated before the Act's effective date (i.e. 3 February 2017) and 12 years post effective date. - The Value Added Tax Act's Record Keeping Regulations (No.1 of 2017) prescribes a retention period of 5 years.

- The Securities and Exchange Commission Rules (2001) provides for a retention period of 5 years (rule n. 7).
- The Inland Revenue Act mandates retention of records of a transaction under the Act for a period of 5 years (Section. 120(6)).
- While the Sri Lankan Telecommunications Act does not mandate a specific retention period, the Telecommunications Regulatory Commission of Sri Lanka ('TRCSL') has imposed the following retention requirements:
    - Mobile operators shall retain Network Address Translation (NAT) records for a period of 3 months;
    - Mobile operators shall retain call detail records (CDRs) for a period of 10 years.

It does not seem to be provided explicitly by legislation of Sri Lanka any explicit possible extension of the retention period.

Limited Retention: Personal information should be kept only as far and as long as necessary for purpose to which it was processed.

3) ADMISSIBILITY OF ELECTRONIC EVIDENCE IN THE CRIMINAL TRIAL

Sri Lanka
What is the requirement under your domestic law for electronic evidence to be admissible in criminal trial?
When the electronic evidence is obtained by issuing a direct request to an overseas SP, the provisions below may facilitate the admission of electronic evidence obtained in this form: - The Evidence (Special Provisions) Act No.14 of 1995, Section 5(1) confirms the admissibility of evidence generated by a computer. Section 7 indicates the requirements for the procedure. - Electronic Transactions Act, No. 19 of 2006, Section 3 and 5 contains provisions that enhance the evidential value of electronic evidence. The Electronic Transactions Act, No. 19 of 2006, contains provisions that enhance the evidential value of electronic evidence. - Section 3 states the following: "No data message, electronic document, electronic record or other communication shall be denied legal recognition, effect, validity or enforceability on the ground that it is in electronic form."

- Section 5 states that legal requirements for information to be presented in its original form shall be deemed to be satisfied where: “there exists a reliable assurance as to the integrity of the information from the time when it was made available in electronic form and the information contained in the data message, electronic document, electronic record or other communication is available and can be used for subsequent reference.”
- Section 21, Chapter V (Rules Governing Evidence) establishes the applicability of the rules of evidence. Due to which any information contained in a data message, or any electronic document, electronic record or other communication— (a) touching any fact in issue or relevant fact; and (b) compiled, received or obtained during the course of any business, trade or profession or other regularly conducted activity, shall be admissible in any proceedings.
- Moreover, Art. 22 - of the same provision- clarifies that nothing contained in the Evidence (Special Provisions) Act, No. 14 of 1995 shall apply to and in relation to any data message, electronic document, electronic record or other document to which the provision of this Act applies.

Additionally, Section 66 and 67 of the Code of Criminal Procedure, relevant to the production of a document located outside Sri Lanka; Section 11 of the Payment Devices Frauds Act, related to duty to assist investigation; Section 24 of the Prevention of Offences Relating to Sports Act, provide the powers of the unit (the indicated provisions are explicated below) but do not prescribe specific formats for the evidence to be admissible. If a court order is used, then it must carry the signature and official seal of the respective Magistrate. If the requisition orders stem from an expert or police officer, then the request must be communicated through official designated channels. (As provided by Section 26, Part III Miscellaneous, Computer Crime Act 2007).
In practice, where information is sought under Section 67(2) of the Code of Criminal Procedure, the request will state the officer to whom the data should be disclosed, where physical copies are sought. At the point of issuance, the identity of the officer should be verified and recorded.
Finally, the fact the e-evidence is not requested through MLA does not mean that the data is for “intelligence only” and not for use “in court”.
Before obtaining e-evidence from another State without an MLAR, the requesting State must be satisfied that:

- They are not committing a criminal offence in the requested State by requesting data directly or the SP is in contravention of a requested State’s law by disclosing data.
- Obtaining e-evidence by non-MLA means will be adequate for the purpose for which it has been sought by the requesting State. For example, production of the

data through non-MLA channels is admissible as evidence if needed for that purpose in the requested State.

4) RECEIVING REQUESTS FOR ELECTRONIC EVIDENCE FROM OTHER STATES

4.1. **Direct requests** from foreign authorities to service providers

4.1.1. Requests for preservation

Sri Lanka
What legal framework(s) is/are applicable, if any?
The Computer Crimes Act, No.24 of 2007, Section 19 which allows a written request to be sent by the police to the SP to preserve for 7 days – and then by applying to a Magistrate for preservation up to 90 days. Pursuant to Section 24, the SP must not disclose the preservation to a user or any other party. Therefore, it is important that any preservation is served immediately, and a court order obtained thereafter for production of the information, before the expiry of 90 days. Further, Prevention of Offences relating to Sports Act, No. 24 of 2019, Section 27 contains a provision related to preservation of information. When there is a risk that such information or data may be lost, destroyed, modified or rendered inaccessible, such member or the authorized person may by written notice require the person in control of such electronic device to ensure that the information or data be preserved for such period not exceeding thirty days as may be specified in such notice. On an application made to a Magistrate having jurisdiction, the period for which the information or data is to be preserved may be extended for such further period, which in the aggregate shall not exceed ninety days.
Are the service providers in your country prohibited from or have limited capacity for executing such requests from foreign authorities?
The Budapest Convention is applicable in this case. According to Article 18, competent Sri Lankan authorities shall be able to order a person in their territory to submit specified computer data in that person's possession; and a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession. Moreover, Article 25 provides for the general principles relating to mutual legal assistance between parties and obliges them to co-

operate for both criminal offences related to computer systems and data and to the collection of electronic evidence for any criminal offence.

If they are prohibited or if there are limitations, are there any alternative options to preserve the data from your country, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or mutual legal assistance (MLA)?

International Treaties:

- Sri Lanka ratified the Council of Europe Convention on Cybercrime (2001) (the 'Budapest Convention'). Article 29 rules explicitly that expedited preservation is always possible.
- The United Nations Convention Against Corruption (2003) Articles 43 and 46: provisions on international cooperation, are also related to preservation of evidence—however, only with regard to request of assistance on corruption-related crimes.
- For Commonwealth States, the Revised Harare Scheme 2011: Paragraphs 21(7) provides for electronic evidence; 24 provides for real-time collection of traffic data; and 23 provides for real-time collection of content.

Section 3 of the Mutual Assistance in Criminal Matters Mutual Assistance in Criminal Matters Act, No. 25 of 2002 and its Amendment Act, No. 24 of 2018 sets the object, which includes 'the tracing of crimes committed via internet, information communications technology, cloud computing, blockchain technology and other computer networks including the trading in of any digital currencies' (Section 3(1)(l)). Section 3 letter (n) states that this Act aims "to facilitate the provision and obtaining by Sri Lanka of assistance in criminal and related matters, including the expedited preservation of stored computer data and expedited disclosure of preserved traffic data and data retention"
Under MACM, Sections 20A to 20D rule expedited preservation of stored data in relation to computer crimes, which enables foreign investigators to obtain the preservation of data in Sri Lanka, in accordance with Sri Lanka's obligations under the Budapest Convention.

Going through police-to-police cooperation or other channels (where direct contact with SPs is not an option), using one of the established 24/7 channel/networks:

- G7 24/7 Network, Council of Europe Budapest 24/7 Network (*ex* Art. 35 of the Budapest Convention) or
- as member state of Interpol, hosts an INTERPOL National Central Bureau (NCB). This connects their national law enforcement with other countries and with the General Secretariat via the Interpol secure global police communications network called I-24/7.

Is a judicial order required from the requesting state?
It is not specifically provided by the law if any judicial order is needed from the requesting state for a data to be preserved in the context of a direct request for preservation made directly to a Service Provider.
Are there any time limits for data preservation? Any possibility of extension?
It is possible for police to require preservation for a period of 7 days, which can be extended up to 90 days following a request issued by a Magistrate (Computer Crimes Act, No. 24 of 2007, Section 18).
Would service providers in your country notify the data subjects of the request?
Even though any specific norm includes a specific regulation related to notification, pursuant to Section 24 of the Computer Crimes Act, No.24 of 2007, the SP must not disclose the preservation to a user or any other party.

4.1.2. Requests for voluntary disclosure

Sri Lanka
What legal framework(s) is/are applicable, if any?
Sri Lankan legislation does not provide an explicit provision in this regard. However, Article 18 of the Budapest Convention, which ensures the right of a State Party to adopt a production order to facilitate the process of obtaining information. This article provides an appropriate legal basis for such assistance, relieving them of any contractual or noncontractual liability for voluntary disclosure of data. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order enforcement of this provision. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control"

Are the service providers in your country prohibited from or have limited capacity for executing such requests from foreign authorities?
No. According to Article 18.b of the Budapest Convention, a Service Provider offering its services in the territory of the Party can submit subscriber information relating to such services in that service provider's possession or control, whether is needed throw the adoption of a production order to empower the authority to reply.
If they are prohibited or if there are limitations, are there any alternative options to preserve the data from your country, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or mutual legal assistance (MLA)?
Going through police-to-police cooperation or other channels (where direct contact with SPs is not an option), using one of the established 24/7 channel/networks G7 24/7 Network, Council of Europe Budapest 24/7 Network (*ex.* Art. 35 of the Budapest Convention) or via the Interpol secure global police communications network called I-24/7. Furthermore, Section 3 (2) of the Mutual Assistance in Criminal Matters Mutual Assistance in Criminal Matters Act, No. 25 of 2002 and its Amendment Act, No. 24 of 2018 states that nothing shall preclude the granting or obtaining of any other form or nature of assistance for investigation in connection with judicial proceedings, connected with criminal matters to or from a specified country or specified organization. Such assistance may include controlled operations, joint investigations, the use of other special investigative techniques including the use of diverse search engines and the transfer of criminal proceedings to another court. This provision extends and, in any case, does not limit the cooperation in investigation on criminal matters also through other form of assistance. Domestic frameworks that implement Article 18 of the Budapest Convention can be found under Section 18 the Computer Crimes Act, No. 24 of 2007 Powers of search and seizure with warrant. This procedural power is especially important to ensure that domestic SPs produce electronic evidence. It includes interception of communications and traffic data real-time. Both can track subjects' comments online and monitor locations through IP addresses or geolocation data. If investigations are urgent and the electronic evidence could be lost, destroyed, modified or rendered inaccessible and confidentiality is required, a police officer or expert can proceed without a warrant. Urgency is not defined; the legal threshold is unknown and the period of interception is not provided.

Under the Code of Criminal Procedure Act, Section 66 provides “summons to produce document or other thing”. It is a relevant provision considering that this section does not grant requisition powers to the Attorney-General or Police. This provision can apply even if the data is located outside Sri Lanka, as the requirement is to have “possession or power” over such document sought. Moreover, this provision can be used when the Service Provider is not a licensed telecom operator, such as a social media provider. Payment Devices Frauds Act Duty to assist investigation. According to Section 11 any person who is required by an expert or a police officer to make any disclosure or to assist in an investigation under this Act, shall comply with such requirement. A person who obstructs the lawful exercise of the powers conferred on an expert or a police officer during an investigation shall be guilty of an offence (to the punishment provided by the Section 11). Prevention of Offences Relating to Sports Act Powers of the Unit. Section 24. This provision can apply even if the data is located outside Sri Lanka, as the requirement is to have “possession or power” over such document sought.
Is a judicial order required from the requesting state? Are there any time limits?
It does not appear to be explicitly regulated.
Would service providers in your country notify the data subjects of the request?
Pursuant to Section 24 of the Computer Crimes Act, No.24 of 2007, the SP must not disclose the preservation to a user or any other party.
How can the process be simplified or quickened in emergency situations?
Any legislation explicitly regulates how the process can be speed up in emergency situations in the case of a direct request to SP. However, under the MACM, the Central Authority of Sri Lanka has an obligation to “prioritize the execution of urgent requests” (Section 4A(c)). The prescribed Mutual Assistance Request Form would still need to be completed, with section 11 addressing the urgency of the request; the reasons for such urgency and the relevant deadlines. Any urgent request can be faxed or emailed, although the hard copy must still be sent.

4.2. Requests received by your central authority for **Mutual Legal Assistance (MLA)**

Sri Lanka

How do you execute MLA requests for electronic evidence stored by domestic service providers (e.g. through a domestic court order or a search warrant)?

The Mutual Assistance in Criminal Matters Act, No. 25 of 2002 and its Amendment Act, No. 24 of 2018 establishes under Section 10 the procedure to transfer electronic evidence stored in Sri Lanka to a foreign authority.

Where the appropriate authority of a specified country makes a request to the Central Authority that an evidence has to be taken in Sri Lanka for the purposes of a proceeding in relation to a criminal matter in the specified country, the Central Authority may, in their discretion, refer such request to a Magistrate. The magistrate, authorized by a general or special order made by the President of the Court of Appeal to take such evidence or to receive such documents or articles, shall, upon receipt of such evidence, documents or articles from such Magistrate, transmit the same to the appropriate authority of the specified country (s.10(1)).

Where the taking of evidence or the production of documents or other articles under subsection (1) has been authorized the Magistrate may require the production before him, of the documents or other articles and, where the documents or other articles are so produced, the Magistrate shall send the documents, or where it is impracticable to send such documents to the Central Authority or where the request relates only to copies of such documents, copies of such documents certified to be true copies by the Magistrate, or the other articles, as the case may be, to the Central Authority. The Central Authority shall cause the certificate of the Magistrate sent to him under subsection (3) to be transmitted to the appropriate authority of the specified country.

The procedure for data production/execution is described under art. 20 of the MLA Act 2020. Under this provision it is established that upon request of a country, the central authority may make an application to the court to issue an order for the production of:

a) specified electronic data in the possession or control of a person which is stored in a computer system and is reasonably believed to be connected with a criminal matter pending in the requesting country; and
b) electronic data in the possession or control of service provider, where such data or information is reasonably believed to be connected to criminal matter pending in the requesting country.

(2) The court may issue a search warrant or order authorizing a person designated by it to search or otherwise access any computer system or part thereof in which computer data may be stored.

(3) The search warrant or order issued pursuant to subsection (1) may authorize the designated person, where necessary, to seize or otherwise, secure an information system or part thereof;

a) make and retain a copy of the electronic data;

b) maintain the integrity of the relevant electronic data; and
c) render inaccessible or remove the electronic data in the accessed information system.

(4) The person in possession of the electronic data or information system sought to be searched, seized or produced, may file an application within fourteen days of notice of an order under subsection (3) objecting to such seizure, copying, retaining or otherwise handing of such electronic data. Provided that until the expiry of the said fourteen days from the date of the notice of the order, the electronic data shall be kept secured and no copies or extracts from the data shall be allowed.

Can you provide assistance in real-time collection of non-content and/or content data (e.g. through electronic surveillance) upon the receipt of a MLA request? If yes, are there any limitations or conditions (e.g. limited to certain crime types or penalties thresholds)?

Under the Budapest Convention art. 33 is affirming the power to provide real-time collection of traffic data to a State Party through mutual legal assistance, which shall be executing according to the domestic law.
At the same time, under article 34 (Interception of content data) is enshrined that Parties shall provide mutual legal assistance to each other in the real-time collection or recording of content data of specified communication transmitted by means of computer system to the extent permitted under their applicable treaties and domestic laws.

According to Section 18 of the 2007 Computer Crime Act An expert or a police officer may investigation under this Act under the authority of a warrant issued in that behalf by a Magistrate obtain any information including subscriber information and traffic data in the possession of any service provider and intercept any wire or electronic communication including subscriber information and traffic data, at any stage of such communication. An expert or a police officer may without a warrant if (a) the investigation needs to be conducted urgently; (b) there is a likelihood of the evidence being lost, destroyed, modified or rendered inaccessible; and (c) there is a need to maintain confidentiality regarding the investigation. The Minister may by regulation prescribe the manner in which and the procedures required to be followed in respect of, the retention and interception of data and information including traffic data, for the purposes of any investigation under the Computer Crime Act.

Under Section 20 of the Computer Crime Act are indicated the power of search and seizure and the relevant procedure, applicable on any electronic device.

What are the central and competent authorities in your country to:

a) **Receive a request for MLA in criminal matters?**
b) **Execute/recognize the measure (if other than the receiving authority)?**

The Secretary to the Ministry of Justice and Foreign Affairs, shall be the Central Authority for the purposes of the Mutual Assistance in Criminal Matters (Amendment) Act, No. 24 of 2018, Art. 4. Specifically: the Secretary to the Ministry of the Minister, shall be the Central Authority for the purposes of this Act (hereinafter referred to as the "Central Authority"). The Central Authority may authorize an Additional Secretary, in writing to act on behalf of the Central Authority for the purpose of this Act. The Central Authority shall designate competent authorities who shall process information to requests as directed by the Central Authority. Where the Central Authority is unable to carry out his duties on account of ill health or other infirmity or being convicted of an offence, the Minister shall appoint an Additional Secretary to administer the Act, within three days of such inability. Same authority for execution.
What are the accepted languages for MLA requests?
English, Sinhala/Tamil
Can the request be submitted electronically to the central authority?
It seems to be possible according to the information provided by the government website (https://www.moj.gov.lk/index.php?option=com_content&view=article&id=123:mutual-legal-asst&catid=2&Itemid=241&lang=si)
Can the request be submitted directly to the central authority?
Yes, according to Section 4A of the Mutual Assistance in Criminal Matters (Amendment) Act, No. 24 of 2018, due to which the Central Authority shall take all reasonable steps to ensure prompt action in respect of all requests, together with the assistance of such other entities or persons, as may be necessary.
What are the specific requirements (e.g. dual criminality, minimum penalty thresholds, etc.) that the requesting states have to meet under your domestic laws for MLA requests seeking for the provision of electronic evidence?
The Mutual Assistance in Criminal Matters Act, No. 25 of 2002 ('MACM'), as amended by the Mutual Assistance in Criminal Matters (Amendment) Act, No. 24 of 2018 will apply to those States the Minister of Justice declares, by Order published in the Gazette, that are party to an International Convention that Sri Lanka is also a party to, have entered into a Mutual Legal Assistance Treaty (MLAT) with**,** or on the basis of

reciprocity**.** The Minister has declared that the provisions of the Act are applicable to any country that is a party to the following: - The United Nations Convention Against Corruption (2003); - The Council of Europe Convention on Cybercrime (2001) (the 'Budapest Convention'); - A member of the Commonwealth. For countries who have not ratified nor implemented the above-mentioned instruments, the following legal framework(s) can be applicable: - 2000 United Nations Convention against Transnational Organized Crime (Palermo Convention); - Other bilateral treaties; Other multilateral treaties (Sri Lanka is a party to 11 of the nineteen global anti-terrorism legal instruments). Part 1 of Section 6 of the MACM, indicates the grounds for refuse assistance. Specifically: dual criminality; the punishment is for an offence of a political character; within Sri Lankan legal framework would constitute a military offence; the person has been acquitted by the Sri Lankan system; sharing the information might be prejudicial to national security, international relationship or public policy; compliance with the request would facilitate the violation of the core human rights of the person.

5) REQUESTING ELECTRONIC EVIDENCE ACROSS BORDERS

5.1. **Direct requests** to foreign service providers

5.1.1. Requests for preservation

Sri Lanka
What legal framework(s) is/are applicable, if any?
In Sri Lanka the following measures are possible, under the Budapest Convention to require expedited preservation (Art. 29). The 2007 Computer Crime Act provides for domestic powers and procedures for executing the preservation and disclosure of information.
Which authority(ies) in your country is/are allowed to request data preservation to foreign service providers?

Under Sri Lanka's legislation it is possible to preserve e-evidence directly from SPs in another State by law enforcement, prosecutorial or judicial authorities. This is possible according to the Budapest Convention and to the Computer Crime Act, Section 19. This provision indicates that a police officer or expert (Expert is defined in section 17 of the Computer Crimes Act, No.24 of 2007) may give written notice to a person in control of a computer or computer system to preserve specified information or relevance to a criminal investigation for a period of 7 days.
If the requested foreign service providers are prohibited or limited to preserve the data, are there any alternative options to preserve the data, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or MLA?
The execution of the requests for data preservation and disclosure to the State Parties of the Budapest Convention by Sri Lanka appears to be possible via its 24/7 Network in Sri Lanka. Going through police-to-police cooperation or other channels (where direct contact with SPs is not an option), using one of the established 24/7 networks: G7 24/7 Network, Council of Europe Budapest 24/7 Network or 24/7 INTERPOL Network. In the absence of bilateral/multilateral agreements on mutual legal assistance, the options to base the sending or receiving of requests on for retained data is based on reciprocity.The MACM Act, indeed, shall apply also to a country which has not entered into any agreement with Sri Lanka, where the Minister may determine that it is in the best interests of the sovereign nations that Sri Lanka extends and obtains assistance on the basis of reciprocity.
Can a court order or a search warrant be issued for data preservation by foreign service providers? If not, what are the reasons?
To issue a request of preservation of evidence directly to a foreign service provider an application for a Court order may then be made to a Magistrate to extend it for a further period up to 90 days [according to the Computer Crime Act, at Section 19]. Moreover, according to the Code of Criminal Procedures Act provides that a Magistrate shall assist the conduct of an investigation by making and issuing appropriate orders, which could include a preservation (Section 124): "Every Magistrate to whom application is made in that behalf shall assist the conduct of an investigation by making and issuing appropriate orders and processes of court…."

5.1.2. Requests for voluntary disclosure

Sri Lanka
What legal framework(s) is/are applicable, if any?
The law does not seem to provide any specific framework in this regard. However, it always as to be considered the framework of sharing spontaneously information based on Art. 18 and 26 of Budapest Convention or Art. 18(4) and (5) of the United Nations Convention against Transnational Organized Crime)
Which authority(ies) in your country is/are allowed to request data disclosure to foreign service providers?
Data disclosure requests may be being made through personnel contact with foreign service providers.
If the requested foreign service providers are prohibited or limited to voluntarily disclose the data, are there any alternative options to obtain the data, e.g. through police-to-police cooperation, specialized networks (e.g. G7/8 24/7 Network) or MLA?
Using one of the established 24/7 channel/networks G7 24/7 Network, Council of Europe Budapest 24/7 Network (*ex* Art. 35 of the Budapest Convention) or via the Interpol secure global police communications network called I-24/7. Furthermore, Section 3 (2) of the Mutual Assistance in Criminal Matters Mutual Assistance in Criminal Matters Act, No. 25 of 2002 and its Amendment Act, No. 24 of 2018 which states that nothing shall preclude the granting or obtaining of any other form or nature of assistance for investigation in connection with judicial proceedings, connected with criminal matters to or from a specified country or specified organization.
Can a court order or a search warrant be issued for data disclosure by foreign service providers? If not, what are the reasons?
It is not explicitly provided by the law.

5.2. Requests sent by your central authority for **Mutual Legal Assistance (MLA)**

UNODC
United Nations Office on Drugs and Crime

Sri Lanka
What is your central authority to send requests for MLA in criminal matters?
The Secretary of the Ministry of Justice is the Central Authority for Mutual Legal Assistance. Mailing address: Secretary, Ministry of Justice and Prison Reforms Superior Courts Complex, Adhikarana Mawatha, Colombo 12, Sri Lanka. Fax : +94 112 445 447 Email : secretary@moj.gov.lk
Are informal contacts with the central authority of the requested states allowed and used?
Informal personnel contact with the central authority of requested states may occur.