TONGA

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 27 March 2020

[reference to the provisions of the Budapest Convention]

This profile has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of sharing information on cybercrime legislation and assessing the current state of implementation of the Budapest Convention on Cybercrime under national legislation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	N/A
Ratification/accession:	09/05/2017

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter I – Use of terms	
Article 1 – "Computer system", "computer data", "service provider", "traffic data": For the purposes of this Convention: a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data; b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; c "service provider" means: i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service; d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service	*The Computer Crime Act 2003 (to be replaced by the Computer Crimes Bill 2017)* **Sect. 2 Interpretation** In this Act, unless the context otherwise requires: "**computer**" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include; (a) an automated typewriter or typesetter; (b) a portable hand held calculator; or (c) a similar device which is non-programmable or which does not contain any data storage facility; (d) such other device as the Minister may, by notification in the Gazette, prescribe; "**computer data**" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function; "**computer data storage medium**" means any article or material such as a disk, from which information is capable of being reproduced, with or without the aid of any other article or device; "**computer system**" means a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function; "**hinder**", in relation to a computer system, means: (a) cutting the electricity supply to a computer system; (b) causing electromagnetic interference to a computer system;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) corrupting a computer system by any means; and (d) inputting, deleting or altering computer data; "**seize**" includes: (a) make and retain a copy of computer data, including using on site equipment; (b) render inaccessible, or remove, a computer, computer data in the accessed computer system; and (c) take a printout of computer data; "**service provider**" means a public or private entity that provides to users of its services the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of that entity or those users; and "**traffic data**" means computer data that relates to a communication by means of a computer system; and is generated by a computer system that is part of the chain of communication, and shows the communication's origin, destination, route, time, date, size, duration or the type of underlying services.
Chapter II – Measures to be taken at the national level	
Section 1 – Substantive criminal law	
Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems	
Article 2 – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	*The Computer Crime Act 2003 (to be replaced by the Computer Crimes Bill 2017)* **Sect. 4** (1) For the purposes of this section, a computer shall be treated as a "protected computer" if the person committing the offence knew, or ought reasonably to have known, that the computer or program or data is used directly in connection with or necessary for — (a) the security, defense or international relations of the Kingdom; (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or (d) the protection of public safety including system related to essential emergency services. (2) A person who willfully, without lawful excuse, accesses any computer system

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	commits an offence and shall be liable upon conviction to, a fine not exceeding $10,000 or imprisonment for a period not exceeding 2 years or to both. (3) A person who willfully, without lawful excuse, accesses any protected computer commits an offence and shall be liable upon conviction to a fine not exceeding $100,000 or to imprisonment for a period not exceeding 20 years or to both.
Article 3 – Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	*The Computer Crime Act 2003 (to be replaced by the Computer Crimes Bill 2017)* **Sect. 7 - Illegal interception of data** A person who, willfully without lawful excuse, intercepts by technical means: (a) any transmission to, from or within a computer system; or (b) electromagnetic emissions from a computer system that are carrying computer data, commits an offence and shall be liable upon conviction, to a fine not exceeding $5,000 or imprisonment for a period not exceeding 1 year or to both.
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 5 - Interfering with data** A person who, willfully or recklessly without lawful excuse: (a) destroys or alters data; (b) renders data meaningless, useless or ineffective; (c) obstructs, interrupts or interferes with the lawful use of data; (d) obstructs, interrupts or interferes with any person in the lawful use of data; or (e) denies access to data to any person entitled to it; commits an offence and shall be liable upon conviction, to a fine not exceeding $10,000 or to imprisonment for a period not exceeding 2 years or to both.
Article 5 – System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 6 - Interfering with computer system** A person who willfully or recklessly, without lawful excuse: (a) hinders or interferes with the functioning of a computer system; or (b) hinders or interferes with a person who is lawfully using or operating a computer system, commits an offence and shall be liable upon conviction to a fine not exceeding $5,000 or imprisonment for a period not exceeding 1 year or to both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 8 – Illegal devices** (1) A person who: (a) willfully or recklessly, without lawful excuse, produces, sells, procures for use, imports, exports, distributes or makes available: (i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act; or (ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act; or (b) has an item mentioned in subparagraph (i) or (ii) in his possession with the intent that it be used by any person for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act; commits an offence and shall be liable upon conviction to a fine not exceeding $20,000 or imprisonment for a period not exceeding 4 years or to both. (2) A person who possesses more than one item mentioned in subsection (1) subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence under sections 4, 5, 6, or 7 of this Act.
Title 2 – Computer-related offences	
Article 7 – Computer-related forgery Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent	s.170-172 of Criminal Offences Act [Tentative Sect. 10 of the new Computer Crimes Bill]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	
Article 8 – Computer-related fraud Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a any input, alteration, deletion or suppression of computer data; b any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	s.143-145,s.158-159,s.162,164,166,167,168 and 169 of Criminal Offences Act [Tentative Sect. 11 of the new Computer Crimes Bill]
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:	***CRIMINAL OFFENCES (AMENDMENT) ACT 2003 No. 6 of 2003*** 1. (1) This Act may be cited as the Criminal Offences (Amendment) Act, 2003. (2) The Criminal Offences Act (Cap. 18), as amended, is referred to in this Act as the Principal Act. 2. The Principal Act is amended by inserting the following new section after section 115 — 115A Child pornography (1) Any person who, wilfully in any manner — (a) publishes child pornography; (b) produces child pornography for any purpose; or (c) possesses child pornography: commits an offence punishable, upon conviction: (i) in the case of an individual, by a fine not exceeding $100,000 or imprisonment for a period not exceeding 10 years; or (ii) in the case of a corporation by a fine not exceeding $250,000. (2) It is a defence to a charge of an offence under subsections (1)(a) or (1)(c) if

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct; c realistic images representing a minor engaged in sexually explicit conduct 3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	the person establishes that the child pornography was a bona fide scientific, research, medical or law enforcement purpose. (3) For the purposes of this section — (a) the expression "child pornography" includes material that visually depicts — (i) a child engaged in sexually explicit conduct; (ii) a person who appears to be a child engaged in sexually explicit conduct; or (iii) images representing a child engaged in sexually explicit conduct; (b) the expression "child" means a person under the age of 14 years; (c) the expression "publish" includes to — (i) distribute, transmit, disseminate, circulate, deliver, exhibit, lend for gain, exchange, barter, sell or offer for sale, let on hire or offer to let on hire, offer in any other way, or make available in any way; (ii) have in possession or custody, or under control, for the purpose of doing an act referred to in sub-section (1); or (iii) print, photograph, copy or make in any other manner (whether of the same or of a different kind or nature) for the purpose of doing an act referred to in subsection. [Section 115A of the Criminal Offences Act (the existing child pornography offence) defines a child as "a person under the age of 14 years". This is to be amended with the Computer Crimes Bill 2016 to persons under the age of 18 years to follow international norms.]
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral	Copyright act of 2002 but not yet in force yet.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	
Title 5 – Ancillary liability and sanctions	
Article 11 – Attempt and aiding or abetting 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	.
Article 12 – Corporate liability 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal	[Tentative Sect. 14 of the new Computer Crimes Bill]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	
Article 13 – Sanctions and measures 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty. 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.	
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2	***EVIDENCE (AMENDMENT) ACT 2003 No. 21*** **1. Short title** (1) This Act may be cited as the Evidence (Amendment) Act, 2003. (2) The Evidence Act (Cap. 15) as amended, is in this Act referred to as the Principal Act. **2. Interpretation** Section 2 of the Principal Act is amended by inserting the following. ""**data**" means representations, in any form of information or concepts;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
through 11 of this Convention; b other criminal offences committed by means of a computer system; and c the collection of evidence in electronic form of a criminal offence. 3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20. b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system: i is being operated for the benefit of a closed group of users, and ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21	"**electronic record**" means data that is recorded or stored on any medium in or by a computer system or other similar device that can be read or perceived by a person or a computer system or other similar device including a display, printout or other output of that data; "**electronic record system**" includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording and preservation of electronic records." **3. Amendment to section 54** The Principal Act is amended by inserting the following new sections after section 54 — **"54A General admissibility** Nothing in the rules of evidence shall apply to deny the admissibility of an electronic record in evidence on the ground that it is an electronic record. **54B Scope** A court may have regard to evidence adduced under section 54A in applying any law relating to the admissibility of records. **54C Authentication** The person seeking to introduce an electronic record in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be. **54D Best evidence rule** (1) In any legal proceeding, where the best evidence rule is applicable in respect of electronic record, the rule is satisfied on proof of the integrity of the electronic records system in or by which the data was recorded or stored. (2) In any legal proceeding, where an electronic record in the form of printout has been manifestly or consistently acted on, relied upon, or used as the record of the information recorded or stored on the printout, the printout is the record for the purposes of the best evidence rule. **54E Presumption of integrity** In the absence of evidence to the contrary, the integrity of the electronic records system in which an electronic record is recorded or stored is presumed in any legal proceeding — (a) where evidence is adduced that supports a finding that at all material times the computer system or other similar device was operating properly, or if not, that in any respect in which it was not operating properly or out of operation, the integrity of the record was not affected by such circumstances, and there are no other reasonable grounds to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	doubt the integrity of the record; (b) where it is established that the electronic record was recorded or stored by a party to the proceedings who is adverse in interest to the party seeking to introduce it; or (c) where it is established that the electronic record was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not record or store it under the control of the party seeking to introduce the record. **54F Standards** For the purpose of determination under any rule or law whether an electronic record is admissible, evidence may be presented in respect of any standard, procedure, usage or practice on how electronic records are to be recorded or preserved, having regard to the type of business that used, recorded or preserved the electronic record and the nature and purpose of the electronic record. **54G Proof by affidavit** Subject to the provisions of this Act, the matters referred to in sections 54D, 54E and 54F may be established by affidavit. **54H Agreement on admissibility** An agreement between the parties on admissibility of an electronic record does not render the record admissible in a criminal proceeding on behalf of the prosecution, if at the time the agreement was made, the accused person or any of the persons accused in the proceeding was not represented by a law practitioner. **54I Admissibility of electronic signature** For the purposes of this section, — (1) "electronic signature" means any letters, characters, numbers or other symbols in electronic form attached to or logically associated with an electronic record, and executed or adopted with the intention of authenticating or approving the electronic record. (2) Where a rule of evidence requires an electronic signature, or provides for certain consequences if a document is not signed, an electronic signature satisfies that rule of law or avoids those consequences. (3) An electronic signature may be proved in any manner, including by showing that a procedure existed by which it is necessary for a person, in order to proceed further with a transaction, to have executed a symbol or security procedure for the purpose of verifying that an electronic record is that of the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	person."
Article 15 – Conditions and safeguards 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 13 Preservation of data** (1) Where any police officer is satisfied that: (a) data stored in a computer system is reasonably required for the purpose of a criminal investigation; and (b) there is a risk that the data may be destroyed or rendered inaccessible; the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice. (2) The Magistrate may upon application authorize an extension not exceeding 14 days. [Tentative Sect. 20 of the new Computer Crimes Bill]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
Article 17 – Expedited preservation and partial disclosure of traffic data 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 12 Disclosure of traffic data** Where a magistrate is satisfied on the basis of an application by any police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify: (a) the service providers; and (b) the path through which the communication was transmitted. [Tentative Sect. 19 of the new Computer Crimes Bill]
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b 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 or control.	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 13 Preservation of data** (1) Where any police officer is satisfied that: (a) data stored in a computer system is reasonably required for the purpose of a criminal investigation; and (b) there is a risk that the data may be destroyed or rendered inaccessible; the police officer may, by written notice given to a person in control of the computer system, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	(2) The Magistrate may upon application authorize an extension not exceeding 14 days. **Sect. 17 Confidentiality and limitation of liability** (1) An Internet service provider who without lawful authority discloses: (a) the fact that an order under sections 11, 12, 13, 14 and 15 has been made; (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence and shall be liable upon conviction to a fine not exceeding $50,000 or imprisonment for a period not exceeding 10 years or *to both.* **Sect. 10 Assisting police** (1) A person who is in possession or control of a computer, computer system, computer data or data storage medium that is the subject of a search under section 9 shall permit, and assist if required, the person making the search to — (a) access and use a computer system or computer data storage medium to search any computer data available to or in the system; (b) obtain and copy that computer data; (c) use equipment to make copies; and (d) obtain an intelligible output from a computer system in a format that can be read. (2) A person who fails without lawful excuse to permit or assist a person acting under a search warrant commits an offence and shall be liable upon conviction to a fine not exceeding $10,000 or imprisonment for a period not exceeding 2 years or to both. [Tentative Sect. 18 of the new Computer Crimes Bill]
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 9 Search and seizure warrants** (1) If a magistrate is satisfied on sworn evidence that there are reasonable grounds to suspect that there may be in a place a computer, computer system, computer data or data storage medium which: (a) may be material evidence in proving an offence; or (b) has been acquired by a person as a result of an offence; the magistrate may issue a warrant authorizing any police officer, with such assistance as may be necessary, to enter the place to search and seize the computer, computer system, computer data or data storage medium.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	(2) Any person who makes a search or seizure under this section, shall at the time or as soon as practicable: (a) make a list of what has been seized, with the date and time of seizure; and (b) give a copy of that list to — (i) the occupier of the premises; or (ii) the person in control of the computer system. (3) Subject to subsection (4), on request, any police officer or another authorized person shall: (a) permit a person who had the custody or control of the computer system, or someone acting on their behalf to access and copy computer data on the system; or (b) give the person a copy of the computer data. (4) The police officer or another authorized person may refuse to give access or provide copies if he has reasonable grounds for believing that giving the access, or providing the copies may — (a) constitute a criminal offence; or (b) prejudice: (i) the investigation in connection with which the search was carried out; (ii) another ongoing investigation; or (iii) any criminal proceedings that are pending or that may be brought in relation to any of those investigations. [Tentative Sect. 17 of the new Computer Crimes Bill]
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of,	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 15 Interception of traffic data** (1) Where any police officer is satisfied that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the police officer may, by written notice given to a person in control of such data, request that person to: (a) collect or record traffic data associated with a specified communication during a specified period; and (b) permit and assist a specified police officer to collect or record that data. (2) Where a magistrate is satisfied on the evidence that there are reasonable

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	grounds to suspect that traffic data is reasonably required for the purposes of a criminal investigation, the magistrate may authorize any police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. **Sect. 17 Confidentiality and limitation of liability** (1) An Internet service provider who without lawful authority discloses: (a) the fact that an order under sections 11, 12, 13, 14 and 15 has been made; (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence and shall be liable upon conviction to a fine not exceeding $50,000 or imprisonment for a period not exceeding 10 years or to both. (2) An internet service provider shall not be liable under any law for the disclosure of any data or other information that he discloses under sections, 11, 12, 13, 14, or 15. [Tentative Sect. 22 of the new Computer Crimes Bill]
Article 21 – Interception of content data 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party, or ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 14 Interception of electronic communications** Where a magistrate is satisfied on the evidence that there are reasonable grounds to suspect that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate may: (a) order an internet service provider to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or (b) authorize any police officer to collect or record that data through application of technical means. **Sect. 17 Confidentiality and limitation of liability** (1) An Internet service provider who without lawful authority discloses: (a) the fact that an order under sections 11, 12, 13, 14 and 15 has been made; (b) anything done under the order; or (c) any data collected or recorded under the order; commits an offence and shall be liable upon conviction to a fine not exceeding $50,000 or imprisonment for a period not exceeding 10 years or to both. (2) An internet service provider shall not be liable under any law for the

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
execution of any power provided for in this article and any information relating to it. 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	disclosure of any data or other information that he discloses under sections, 11, 12, 13, 14, or 15. [Tentative Sect. 21 of the new Computer Crimes Bill]
Section 3 – Jurisdiction	
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.	*The Computer Crime Act 2003 (to be replaced by the new Computer Crimes Bill)* **Sect. 3 Jurisdiction** (1) Where an offence under this Act is committed by any person who is outside the Kingdom, he shall be deemed to have committed the offence within the Kingdom. (2) For the purposes of this section, this Act shall apply as if, for the offence in question: (a) the accused; or (b) the computer, program or data was in the Kingdom at the material time. [Tentative Sect. 3 of the new Computer Crimes Bill]
Chapter III – International co-operation	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply. 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article. 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves. 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition. 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party. 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty. b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure	
Article 25 – General principles relating to mutual assistance 1 The Parties shall afford one another mutual assistance to the widest extent possible 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. 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of	[Section 8 of the Mutual Assistance in Criminal Matters Act 2000 (Mutual Assistance Act) allows authorised officers to apply for search warrants or evidence-gathering orders in relation to requests for assistance approved by the Attorney General. However, it is not entirely clear that this application process extends to interception warrants or to preservation orders. Section 7 of the Mutual Assistance Act specifies the information that a foreign state must provide in a request for mutual assistance. The requirement to provide all of this information may be too onerous where there is an urgent need to preserve data.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.	
Article 26 – Spontaneous information 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	***Mutual Assistance in Criminal Matters Act, 2000*** General principles relating to international co-operation (1) The Attorney General may cooperate with any foreign Government, 24 x 7 network, any foreign agency or any international agency for the purposes of investigations or proceedings concerning offences related to computer systems, electronic communication or data or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of a computer system or real-time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provisions under this Act. (2) The Attorney General may make requests on behalf of Tonga to a foreign State for mutual assistance in any investigation commenced or proceeding instituted in Tonga, relating to any serious offence. (3) The Attorney General may, in respect of any request from a foreign State for mutual assistance in any investigation commenced or proceeding instituted in that State relating to a serious offence: (a) grant the request, in whole or in part, on such terms and conditions as he thinks fit; (b) refuse the request, in whole or in part, on the ground that to grant the request would be likely to prejudice the sovereignty, security of Tonga or would otherwise be against the public interest; or (c) after consulting with the appropriate authority of the foreign State, postpone the request, in whole or in part on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in Tonga. (d) postpone action on a request if such action would prejudice an investigation or proceeding in Tonga. (4) The Attorney General may require the foreign Government, 24 x 7 network, any foreign agency or any international agency to: (a) keep the contents and any information and material provided confidential, (b) only use the contents and any information and material provided for

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	the purpose of the criminal matter specified in the request, and (c) use it subject to other conditions. (5) Requests on behalf of Tonga to foreign States for assistance shall be made only by or with the authority of the Attorney General. (6) The Attorney General may, without prior request, forward to such foreign Government, 24 x 7 network, any foreign agency or any international agency, any information obtained from its own investigations if it considers that the disclosure of such information might assist the foreign Government or agency in initiating or carrying out investigations or proceedings concerning any offence. (7) The Attorney General may access publicly available stored computer data, regardless of where the data is located geographically; or access or receive, through a computer system in its territory, stored computer data located outside Tonga, if the Attorney General obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities. 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the	***Mutual Assistance in Criminal Matters Act, 2000*** **Expedited preservation of stored computer data** (1) Subject to Section [General principles relating to international co-operation], a foreign Government, foreign agency or any international agency may request the Attorney General to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
data. 2 A request for preservation made under paragraph 1 shall specify: a the authority seeking the preservation; b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c the stored computer data to be preserved and its relationship to the offence; d any available information identifying the custodian of the stored computer data or the location of the computer system; e the necessity of the preservation; and f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.	Tonga or control of the Government and in respect of which the requesting foreign Government, foreign agency or any international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data. (2) A request for preservation made under sub-section (1) shall specify: (a) the authority seeking the preservation; (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (c) the stored computer data to be preserved and its relationship to the offence; (d) any available information identifying the custodian of the stored computer data or the location of the computer system; (e) the necessity of the preservation; and (f) that the foreign Government, foreign agency or any international agency intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. (3) Upon receiving the request under this section, the Attorney General shall take all appropriate measures to preserve expeditiously the specified data in accordance with the procedures and powers provided under this Act. (4) Any preservation effected in response to the request referred to under this section shall be for a period not less than sixty days, in order to enable the foreign Government, foreign agency or any international agency to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data and following the receipt of such a request, the data shall continue to be preserved until a final decision is taken on that pending request.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
Article 30 – Expedited disclosure of preserved traffic data 1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	***Mutual Assistance in Criminal Matters Act, 2000*** **Expedited disclosure of preserved traffic data** (1) Where during the course of executing a request under Section [Expedited preservation of stored computer data] or otherwise, with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting foreign Government, foreign agency or any international agency a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. (2) Expedited disclosure of preserved traffic data under sub-section (1) may only be withheld if: (a) the request concerns a political offence or an offence related to a political offence; or (b) the requested Party considers that the execution of the request is likely to prejudice its sovereignty, security or public interest.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Mutual Assistance in Criminal Matters Act, 2000 **Mutual assistance regarding accessing of stored computer data** (1) Subject to Section [General principles relating to international co-operation], a foreign Government, foreign agency or any international agency may request the Attorney General to order or otherwise to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Section [Expedited preservation of stored computer data]. (2) A request for mutual assistance regarding accessing of stored computer data shall as far as practicable: (a) give the name of the authority conducting the investigation or proceeding to which the request relates; (b) give a description of the nature of the criminal matter and a statement setting-out a summary of the relevant facts and laws; (c) give a description of the purpose of the request and of the nature of the assistance being sought; (d) in the case of a request to restrain or confiscate assets believed on reasonable grounds to be located in the requested State, give details of the offence in question, particulars of any investigation or proceeding commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order; (e) give details of any procedure that the requesting State wishes to be followed by the requested State in giving effect to the request, particularly in the case of a request to take evidence; (f) include a statement setting-out any wishes of the requesting State concerning any confidentiality relating to the request and the reasons for those wishes; (g) give details of the period within which the requesting State wishes the request to be complied with; (h) where applicable, give details of the property, computer, computer system or electronic device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in the requested State; (i) give details of the stored computer data, data or program to be seized and its relationship to the offence; (j) give any available information identifying the custodian of the stored

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	computer data or the location of the computer, computer system or electronic device; (k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and (l) give any other information that may assist in giving effect to the request. (3) Upon receiving the request under this section, the Attorney General shall take all appropriate measures to obtain necessary authorization including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act. (4) Upon obtaining necessary authorization including any warrants to execute upon the request, the Attorney General may seek the support and cooperation of the foreign Government, foreign agency or any international agency during the search and seizure.
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	***Mutual Assistance in Criminal Matters Act, 2000*** **General principles relating to international co-operation** (1) The Attorney General may cooperate with any foreign Government, 24 x 7 network, any foreign agency or any international agency for the purposes of investigations or proceedings concerning offences related to computer systems, electronic communication or data or for the collection of evidence in electronic form of an offence or obtaining expeditious preservation and disclosure of traffic data or data by means of a computer system or real-time collection of traffic data associated with specified communications or interception of content data or any other means, power, function or provisions under this Act. (2) The Attorney General may make requests on behalf of Tonga to a foreign State for mutual assistance in any investigation commenced or proceeding instituted in Tonga, relating to any serious offence. (3) The Attorney General may, in respect of any request from a foreign State for mutual assistance in any investigation commenced or proceeding instituted in that State relating to a serious offence: (a) grant the request, in whole or in part, on such terms and conditions as he thinks fit; (b) refuse the request, in whole or in part, on the ground that to grant the request would be likely to prejudice the sovereignty, security of Tonga or would otherwise be against the public interest; or (c) after consulting with the appropriate authority of the foreign State,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	postpone the request, in whole or in part on the ground that granting the request immediately would be likely to prejudice the conduct of an investigation or proceeding in Tonga. (d) postpone action on a request if such action would prejudice an investigation or proceeding in Tonga. (4) The Attorney General may require the foreign Government, 24 x 7 network, any foreign agency or any international agency to: (a) keep the contents and any information and material provided confidential, (b) only use the contents and any information and material provided for the purpose of the criminal matter specified in the request, and (c) use it subject to other conditions. (5) Requests on behalf of Tonga to foreign States for assistance shall be made only by or with the authority of the Attorney General. (6) The Attorney General may, without prior request, forward to such foreign Government, 24 x 7 network, any foreign agency or any international agency, any information obtained from its own investigations if it considers that the disclosure of such information might assist the foreign Government or agency in initiating or carrying out investigations or proceedings concerning any offence. (7) The Attorney General may access publicly available stored computer data, regardless of where the data is located geographically; or access or receive, through a computer system in its territory, stored computer data located outside Tonga, if the Attorney General obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data through that computer system.
Article 33 – Mutual assistance in the real-time collection of traffic data 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	***Mutual Assistance in Criminal Matters Act, 2000*** **Mutual assistance regarding the real-time collection of traffic data** (1) Subject to Section [General principles relating to international co-operation], a foreign Government, foreign agency or any international agency may request the Attorney General to order or otherwise provide assistance in real-time collection of traffic data associated with specified communications in the territory of Tonga transmitted by means of a computer system. (2) A request for assistance under this section shall so far as practicable specify: (i) the authority seeking the use of powers under this section; (ii) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(iii)the name of the authority with access to the relevant traffic data; (iv) the location at which the traffic data may be held; (v) the intended purpose for the required traffic data; (vi) sufficient information to identify the traffic data; (vii) any further details relevant traffic data; (viii) the necessity for use of powers under this section; and (ix) the terms for the use and disclosure of the traffic data to third parties. (3) Upon receiving the request under this section, the Attorney General shall take all appropriate measures to obtain necessary authorization including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act. (4) Upon obtaining necessary authorization including any warrants to execute upon the request, the Attorney General may seek the support and cooperation of the foreign Government, foreign agency or any international agency during the search and seizure. (5) Upon conducting the measures under this section the Attorney General shall subject to Section [General principles relating to international co-operation], provide the results of such measures as well as real-time collection of traffic data associated with specified communications to the foreign Government, foreign agency or any international agency.
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	***Mutual Assistance in Criminal Matters Act, 2000*** **Mutual assistance regarding the interception of content data** (1) Subject to Section [General principles relating to international co-operation], a foreign Government, foreign agency or any international agency may request the Attorney General to order or otherwise provide assistance in the real-time collection or recording of content data of specified communications transmitted by means of a computer system in the territory of Tonga transmitted by means of a computer system. (2) A request for assistance under this section shall so far as practicable specify: (a) the authority seeking the use of powers under this section; (b) the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; (c) the name of the authority with access to the relevant communication; (d) the location at which or nature of the communication; (e) the intended purpose for the required communication;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(f) sufficient information to identify the communications; (g) details of the data of the relevant interception; (h) the recipient of the communication; (i) the intended duration for the use of the communication; (j) the necessity for use of powers under this section; and (k) the terms for the use and disclosure of the communication to third parties. (3) Upon receiving the request under this section, the Attorney General shall, if the request is in relation to an offence punishable with at least five years imprisonment, take all appropriate measures to obtain necessary authorization including any warrants to execute upon the request in accordance with the procedures and powers provided under this Act. (4) Upon obtaining necessary authorization including any warrants to execute upon the request, the Attorney General may seek the support and cooperation of the foreign Government, foreign agency or any international agency during the search and seizure. (5) Upon conducting the measures under this section the Attorney General shall subject to Section [General principles relating to international co-operation], provide the results of such measures as well as real-time collection or recording of content data of specified communications to the foreign Government, foreign agency or any international agency. (6) The Attorney General may only authorize requests for provision of intercepted content data if the request relates to a serious offence which is punishable by imprisonment for at least 5 years.
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-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. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects.	***Mutual Assistance in Criminal Matters Act, 2000*** **24/7 Network** (1) The Attorney General shall designate a point of contact available on a twenty-four hour, seven-day-a-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, which assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: (a) the provision of technical advice; (b) the preservation of data pursuant to Expedited preservation of stored computer data and Expedited disclosure of preserved traffic data;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis. 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	(c) the collection of evidence, the provision of legal information, and locating of suspects.
Article 42 – Reservations By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.	

Back to the Table of Contents