Bahamas

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version [27.03.2020]

[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.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

State:	
Signature of the Budapest Convention:	No
Ratification/accession:	No

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	**Computer Misuse Act 2003** **Section 2. Interpretation** (1) In this Act — **"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; (c) a similar device which is nonprogrammable or which does not contain any data storage facility; or (d) such other device as the Minister may, by notice published in the Gazette, prescribe; **"computer output" or "output"** means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact — (a) produced by a computer; or (b) accurately translated from a statement or representation so produced; **"computer service"** includes computer time, data processing and the storage or retrieval of data;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"damage" means, except for the purposes of section 12, any impairment to a computer or the integrity or availability of data, a program or system, or information, that — (a) causes economic loss aggregating ten thousand dollars in value, or such other amount as the Minister may, by notice published in the Gazette, prescribe except that any such loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account; (b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons; (c) causes or threatens physical injury or death to any person; (d) threatens public health or public safety; or (e) threatens physical damage to a computer; **"data"** means representations of information or of concepts in a form suitable for use in a computer; **"electronic, acoustic, mechanical or other device"** means any device or apparatus that is used or is capable of being used to intercept any function of a computer; **"function"** includes logic, control, arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a computer; **"intercept",** in relation to a function of a computer, includes listening to or recording a function of a computer, or acquiring the substance, meaning or purport thereof; **"program" or "computer program"** means data representing instructions or statements that, when executed in a computer, causes the computer to perform a function; and a reference in this Act to a program includes a reference to part of a program. (2) For the purposes of this Act, a person "secures access" to any program or data held in a computer if he causes a computer to perform any function in relation to such program or data, that — (a) alters or erases it; (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) uses it; or (d) causes it to be output from the computer in which it is held (whether by having it displayed or in any other manner), and references in this Act to securing access or to an intent to secure such access shall be construed accordingly. (3) For the purposes of subsection (2) (c), a person "uses" a program if the function he causes the computer to perform causes the program to be executed or is itself a function of the program. (4) For the purposes of subsection (2) (d), the form in which any program or data is output is immaterial (including in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a computer). (5) For the purposes of this Act, access of any kind by any person to any program or data held in a computer is "unauthorised" if — (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to such access from any person who is so entitled. (6) A reference in this Act to "any program or data held in a computer" includes a reference to such program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium. (7) For the purposes of this Act, a "modification of the contents of any computer" takes place if, by the operation of any function of the computer concerned or any other computer — (a) any program or data held in the computer concerned is altered or erased; (b) any program or data is added to its contents; or (c) any act occurs which impairs the normal operation of any computer, and any act which contributes towards causing such a modification shall be regarded as causing it. (8) Any modification referred to in subsection (7) is unauthorised if — (a) the person whose act causes it is not himself entitled to determine whether the modification should be made; and

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) he does not have consent to the modification from any person who is so entitled.
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.	**Computer Misuse Act 2003** **Section 3. Unauthorised access to computer material.** (1) Subject to subsection (2), any person who, without authority, knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in any computer shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding six months or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding one year or to both such fine and imprisonment. (2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment. (3) For the purposes of this section, it is immaterial that the act in question is not directed at — (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer. **Section 4. Access with intent to commit or facilitate commission of offence.** (1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	commit an offence (whether by himself or by any other person) to which this section applies shall be guilty of an offence. (2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than two years. (3) Any person guilty of an offence under this section shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment. (4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible. (5) For the purposes of this section, it is immaterial whether — (a) the access referred to in subsection (1) is authorised or unauthorised; (b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.
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.	**Computer Misuse Act 2003** **Section 6. Unauthorised use or interception of computer service** (1) Subject to subsection (2), any person who knowingly — (a) secures access without authority to any computer for the purpose of obtaining, directly or indirectly, any computer service; (b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a computer by means of an electro-magnetic, acoustic, mechanical or other device; or (c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	imprisonment for a term not exceeding three years or to both such fine and imprisonment. (2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment. (3) For the purposes of this section, it is immaterial that the unauthorised access or interception is not directed at — (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer.
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.	**Computer Misuse Act 2003** **Section 5. Unauthorised modification of computer material.** (1) Subject to subsection (2), any person who does any act which he knows will cause an unauthorised modification of the contents of any computer shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding one year or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment. (2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment. (3) For the purposes of this section, it is immaterial that the act in question is not directed at — (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular computer. (4) For the purposes of this section, it is immaterial whether an unauthorised modification is, or is intended to be, permanent or merely temporary.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 7 Obstruction of use of. computer (1) Any person who, knowingly and without authority or lawful excuse - (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment. (2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment.
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	**Computer Misuse Act 2003** **Section 7. Unauthorised obstruction of use of computer.** (1) Any person who, knowingly and without authority or lawful excuse — (a) interferes with, or interrupts or obstructs the lawful use of, a computer; or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a computer, shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment. (2) If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding fifty thousand dollars or to imprisonment for a term not exceeding five years or to both such fine and imprisonment.
Article 6 – Misuse of devices	**Computer Misuse Act 2003**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Section 6. Unauthorised use or interception of computer service** (1) Subject to subsection (2), any person who knowingly — (c) uses or causes to be used, directly or indirectly, the computer or any other device for the purpose of committing an offence under paragraph (a) or (b), shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment and, in the case of a second or subsequent conviction, to a fine not exceeding twenty thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment.
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 that it be considered or acted upon for legal purposes as if it were authentic,	**Computer Misuse Act 2003** **Section 4. Access with intent to commit or facilitate commission of offence.**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence (whether by himself or by any other person) to which this section applies shall be guilty of an offence. (2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than two years. (3) Any person guilty of an offence under this section shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment. (4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible. (5) For the purposes of this section, it is immaterial whether — (a) the access referred to in subsection (1) is authorised or unauthorised; (b) the offence to which this section applies is committed at the same time when the access is secured or at any other time. **Penal Code** **TITLE XIV PETTY FRAUDS BY FORGERY AND FALSE COIN** Electronic Communication and Transactions Act PART II Legal recognition and functional equivalency of electronic communications, signatures, contracts and related matters

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Computer Misuse Act 2003** **Section 4. Access with intent to commit or facilitate commission of offence.** (1) Any person who causes a computer to perform any function for the purpose of securing access to any program or data held in any computer with intent to commit an offence (whether by himself or by any other person) to which this section applies shall be guilty of an offence. (2) This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than two years. (3) Any person guilty of an offence under this section shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment. (4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible. (5) For the purposes of this section, it is immaterial whether — (a) the access referred to in subsection (1) is authorised or unauthorised; (b) the offence to which this section applies is committed at the same time when the access is secured or at any other time.
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;	**Penal Code** **TITLE XXXI CRIMINAL PUBLIC NUISANCES** **489 Publication or sale of blasphemous or obscene libel.** Whoever publishes, sells, or offers for sale any blasphemous or obscene book, writing or representation, shall be liable to imprisonment for two years: Provided that no one shall be convicted under this section for publishing any opinion on religious subjects expressed in good faith and in decent language, or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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: 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.	for attempting to establish by arguments used in good faith and conveyed in decent language any opinion on a religious subject.
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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.	**Computer Misuse Act 2003** **Section 10. Incitement, abetments and attempts punishable as full offence** (1) Any person who incites, solicits or abets the commission of or who attempts to commit or does any act preparatory to or in furtherance of the commission of any offence under this Act shall be guilty of that and shall be liable on summary conviction to the punishment offences. provided for the full offence. (2) For an offence to be committed under this section, it is immaterial where the full offence in question took place.
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	**Computer Misuse Act 2003** **Section 9. Enhanced punishment for offences involving protected computers** (1) Where access to any protected computer is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person shall be tried on information and shall be liable on conviction to a fine not exceeding one hundred thousand dollars or to imprisonment for a term not exceeding twenty years or to both such fine and imprisonment. (2) For the purposes of subsection (1), 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, defence or international relations of The Bahamas; (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 systems related to essential emergency services such as police, civil defence and medical services. (3) For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the computer, program or data, an electronic or other warning exhibited to the accused stating that unauthorised

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	access to that computer,program or data attracts an enhanced penalty under this section.
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 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	**Computer Misuse Act 2003** **Section 11 Territorial scope of offences under this Act Ch.77** (1) This section has effect to supplement the provisions of the Penal Code in relation to the jurisdiction of the courts of The Bahamas to try offences which do not take place wholly in The Bahamas. (2) Subject to subsection (3) the provisions of the Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within The Bahamas. (3) Where an offence under this Act is committed by any person in any place outside The Bahamas, he may be dealt with as if the offence had been committed within The Bahamas. (4) For the purposes of this section, this Act shall apply if, for the offence in question. (a) the accused was in The Bahamas at the material time; or (b) the computer, program or data was in The Bahamas at the material time. **Section 12. Commencement of proceedings** (1) Notwithstanding any Act to the contrary prescribing the time limit within which summary proceedingsmay be commenced and subject to subsection (2), proceedings for an offence under this Act may be brought within a period of twelve months from the date on which evidence sufficient in the opinion of the Attorney-General to warrant prosecutions came to his knowledge. (2) No such proceedings shall be brought by virtue of this section more than three years after the commission of the offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(3) For the purposes of this section, a certificate signed by or on behalf of the Attorney General and stating the date on which evidence sufficient in his opinion to warrant the commencement of proceedings came to his knowledge shall be conclusive evidence of that fact. **Section 13. Order for payment of compensation** (1) The court before which a person is convicted of any offence under this Act may make an order against him for the payment by him of a sum to be fixed by the court by way of compensation to any person for any damage caused to his computer, program or data by the offence for which the sentence is passed. (2) Any claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him under an order for compensation, but the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order. (3) An order of compensation under this section shall be recoverable as a civil debt.
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	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	**Electronic Communication and Transaction Act** **Section 11. Retention of electronic communications** (1)Where certain documents, records or information are required by law to be retained, that requirement is met by retaining electronic communications if the following conditions are satisfied — (a)the information contained in the electronic communication is accessible so as to be usable for subsequent reference;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	(b)the electronic 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)any information that enables the identification of the origin and destination of an electronic communication and the date and time when it was sent or received is retained. (2)An obligation to retain documents, records or information in accordance with subsection (1) shall not extend to any information the sole purpose of which is to enable the message to be sent or received. (3)A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions set out in subsection (1) (a), (b)and (c) are met. (4)Nothing in this section shall preclude any public body from specifying additional requirements for the retention of electronic communications that are subject to the jurisdiction of such public body.
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. 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;	**Computer Misuse Act 2003** **Section 16 Power of police officer to access computer and data. Ch. 91.** (1) A police officer or a person authorised in writing by the Commissioner of Police, pursuant to a warrant under section 70 of the Criminal Procedure Code, shall — (a) be entitled at any time to — (i) have access to and inspect and check the operation of any computer to which this section applies; (ii) use or cause to be used any such computer to search any data contained in or available to such computer; or (iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section; (b) be entitled to require — (i) the person by whom or on whose behalf, the police officer or investigation officer has reasonable cause to suspect, any computer to which this section applies is or has been used; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	(ii) any person having charge of, or otherwise concerned with the operation of, such computer, to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); or (c) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence. (2) This section shall apply to a computer which a police officer or a person authorised in writing by the Commissioner of Police has reasonable cause to suspect is or has been in use in connection with any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section. (3) The powers referred to in paragraphs (a) (ii) and (iii) and (c) of subsection (1) shall not be exercised except with the consent of the Attorney-General. (4) Any person who obstructs the lawful exercise of the powers under subsection (1) (a) or who fails to comply with a request under subsection (1) (b) or (c) shall be guilty of an offence and shall be liable on summary conviction to a fine not exceeding ten thousand dollars or to imprisonment for a term not exceeding three years or to both such fine and imprisonment. (5) For the purposes of this section — "decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version; "encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilised for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data; "plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	**Computer Misuse Act 2003** **Section 15 Police powers** (1) A police officer may arrest without warrant any person who has committed or is committing, or whom the police officer with reasonable cause suspects to have committed, or to be committing, an offence under this Act. (2) Any power of seizure conferred on a police officer who has entered premises by virtue of a warrant issued under section 70 of the Criminal Procedure Code in relation to an offence under this Act, or any related inchoate offence, shall be construed as including a power to require any information relating to the warrant which is held in a computer and accessible from the premises to be produced in a form in which it can be taken away and in which it is legible (whether or not with the use of a computer). (3) Where the items seized by a police officer under section 70 of the Criminal Procedure Code include computers, disks or other computer equipment, the magistrate before whom those items are brought in accordance with section 72 of the Criminal Procedure Code may, on the application of the person to whom those items belong or from under whose control they were taken, and subject to subsection (4), make an order — (a) permitting a police officer to make copies of such programs or data held in the computer, disks or other equipment as may be required for the investigation or prosecution of the offence; (b) requiring copies of those copies to be given to any person charged in relation to the offence ("the accused person"); and (c) requiring the items to be returned within a period of seventy-two hours, and when seizing any such items the police officer shall inform the person to whom those items belong or from under whose control they are taken of his right to make an application under this subsection. (4) Subsection (3) (b) shall not apply — **Section 17. Forfeiture**

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(1) Where a person is convicted of an offence under this Act, or any related inchoate offence, and the court is satisfied that any property which was in his possession or under his control at the time he was apprehended for the offence or when a summons in respect of it was issued — (a) has been used for the purpose of committing, or facilitating the commission of, the offence in question or any other such offence; or (b) was intended by him to be used for that purpose, the court may order that property to be forfeited to the Crown, and may do so whether or not it deals with the offender in respect of the offence in any other way. (2) In considering whether to make an order in respect of any property the court shall have regard — (a) to the value of the property; and (b) to the likely financial and other effects on the offender of the making of the order (taken together with any other order the court contemplates making).
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, 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	

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.	
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 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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
Article 24 – Extradition 1 a This article applies to extradition between Parties for the criminal 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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;	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
voluntary consent of the person who has the lawful authority to disclose the data to the Party 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.	
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.	
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. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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