Singapore

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 7 May 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:	
Ratification/accession:	

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 (CHAPTER 50A) PART I PRELIMINARY **Interpretation** 2.—(1) 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; (c) a similar device which is non-programmable or which does not contain any data storage facility; or (d) such other device as the Minister may, by notification 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 13, any impairment to a computer or the integrity or availability of data, a program or system, or information, that — (a) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the Gazette, prescribe except that any 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; or (d) threatens public health or public safety; "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer; "electro-magnetic, acoustic, mechanical or other device" means any device, apparatus or program that is used or is capable of being used to intercept any function of a computer; [Act 22 of 2017 wef 01/06/2017] "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.
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.	PART II OFFENCES **Unauthorised access to computer material** 3.—(1) Subject to subsection (2), any person who knowingly causes a computer to perform any function for the purpose of securing access without authority to any program or data held in any computer shall be guilty of an offence and shall

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both. [21/98] (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 $50,000 or to imprisonment for a term not exceeding 7 years or to both. [21/98] (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. [UK CMA 1990, s. 1] Access with intent to commit or facilitate commission of offence 4.—(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 to which this section applies shall be guilty of an offence. [21/98] (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 2 years. [21/98] (3) Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both. [21/98] (4) 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. [21/98] [UK CMA 1990, s. 2]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Unauthorised modification of computer material 5.—(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 conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both. [21/98] (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 $50,000 or to imprisonment for a term not exceeding 7 years or to both. [21/98] (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. [UK CMA 1990, s. 3]
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.	**Unauthorised use or interception of computer service** 6.—(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 conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both. [21/98]

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(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 $50,000 or to imprisonment for a term not exceeding 7 years or to both. [21/98] (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. [Canada CLAA 1985, s. 301.2 (1)]
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.	**Unauthorised obstruction of use of computer** 7.—(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 conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both. [21/98] (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 $50,000 or to imprisonment for a term not exceeding 7 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	[Same section as previous]
Article 6 – Misuse of devices	**Unauthorised disclosure of access code** 8.—(1) Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or

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.	data held in any computer shall be guilty of an offence if he did so — (a) for any wrongful gain; (b) for any unlawful purpose; or (c) knowing that it is likely to cause wrongful loss to any person. [21/98] (2) Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both.
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 that it be considered or acted upon for legal purposes as if it were authentic,	.

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.	
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.	**Supplying, etc., personal information obtained in contravention of certain provisions** 8A.—(1) A person shall be guilty of an offence if the person, knowing or having reason to believe that any personal information about another person (being an individual) was obtained by an act done in contravention of section 3, 4, 5 or 6 — (a) obtains or retains the personal information; or (b) supplies, offers to supply, transmits or makes available, by any means the personal information. (2) It is not an offence under subsection (1)(a) if the person obtained or retained the personal information for a purpose other than — (a) for use in committing, or in facilitating the commission of, any offence under any written law; or (b) for supply, transmission or making available by any means for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law. (3) It is not an offence under subsection (1)(b) if — (a) the person did the act for a purpose other than for the personal information to be used in committing, or in facilitating the commission of, any offence under any written law; and (b) the person did not know or have reason to believe that the personal information will be or is likely to be used to commit, or facilitate the commission of, any offence under any written law. Example 1.— A comes across a list of credit card numbers on the Internet belonging to individuals who are customers of B, which A has reason to believe were obtained by securing access without authority to B's server. A downloads the list for the purpose of reporting the unauthorised access to B's server to the police. A retains the list of credit card numbers and transmits it to B for the purpose of informing B of the unauthorised access to B's server.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	A has downloaded and retained the list of credit card numbers for purposes other than those mentioned in subsection (2)(a) and (b). Therefore A does not commit an offence under subsection (1)(a) by reason of subsection (2). A has transmitted the list to B for a purpose other than for it to be used in committing or in facilitating the commission of an offence. If A did not know or have reason to believe that the list so transmitted will be or is likely to be used to commit or facilitate the commission of an offence, then A does not commit an offence under subsection (1)(b) by reason of subsection (3). Example 2.— C, an employee of B, after receiving the list from A in Example 1, transmits it to D, another employee of B, for the purpose of facilitating B's investigation of the unauthorised access of B's server. C has transmitted the list to D for a purpose other than for it to be used in committing or in facilitating the commission of an offence. If C did not know or have reason to believe that the list so transmitted will be or is likely to be used to commit or facilitate the commission of an offence, then C does not commit an offence under subsection (1)(b) by reason of subsection (3). (4) For the purposes of subsection (1)(b), a person does not transmit or make available personal information merely because the person provides, or operates facilities for network access, or provides services relating to, or provides connections for, the transmission or routing of data. (5) A person guilty of an offence under subsection (1) shall be liable on conviction — (a) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and (b) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both. (6) For the purpose of proving under subsection (1) that a person knows or has reason to believe that any personal information was obtained by an act done in contravention of section 3, 4, 5 or 6, it is not necessary for the prosecution to prove the particulars of the contravention, such as who carried out the contravention and when it took place. (7) In this section — (a) personal information is any information, whether true or not, about an individual of a type that is commonly used alone or in combination with other information to identify or purport to identify an individual, including (but not

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	limited to) biometric data, name, address, date of birth, national registration identity card number, passport number, a written, electronic or digital signature, user authentication code, credit card or debit card number, and password; and (b) a reference to an offence under any written law includes an offence under subsection (1). [Act 22 of 2017 wef 01/06/2017] **Obtaining, etc., items for use in certain offences** 8B.—(1) A person shall be guilty of an offence if the person — (a) obtains or retains any item to which this section applies — (i) intending to use it to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7; or (ii) with a view to it being supplied or made available, by any means for use in committing, or in facilitating the commission of, any of those offences; or (b) makes, supplies, offers to supply or makes available, by any means any item to which this section applies, intending it to be used to commit, or facilitate the commission of, an offence under section 3, 4, 5, 6 or 7. (2) This section applies to the following items: (a) any device, including a computer program, that is designed or adapted primarily, or is capable of being used, for the purpose of committing an offence under section 3, 4, 5, 6 or 7; (b) a password, an access code, or similar data by which the whole or any part of a computer is capable of being accessed. (3) A person guilty of an offence under subsection (1) shall be liable on conviction — (a) to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both; and (b) in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both. [Act 22 of 2017 wef 01/06/2017]
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography	

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, 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: 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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	
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.	CONSTITUTION OF THE REPUBLIC OF SINGAPORE PART IV FUNDAMENTAL LIBERTIES **Liberty of the person** 9.—(1) No person shall be deprived of his life or personal liberty save in accordance with law. (2) Where a complaint is made to the High Court or any Judge thereof that a person is being unlawfully detained, the Court shall inquire into the complaint and,

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	unless satisfied that the detention is lawful, shall order him to be produced before the Court and release him. (3) Where a person is arrested, he shall be informed as soon as may be of the grounds of his arrest and shall be allowed to consult and be defended by a legal practitioner of his choice. (4) Where a person is arrested and not released, he shall, without unreasonable delay, and in any case within 48 hours (excluding the time of any necessary journey), be produced before a Magistrate, in person or by way of video-conferencing link (or other similar technology) in accordance with law, and shall not be further detained in custody without the Magistrate's authority. [9/2010 wef 01/07/2010] (5) Clauses (3) and (4) shall not apply to an enemy alien or to any person arrested for contempt of Parliament pursuant to a warrant issued under the hand of the Speaker. (6) Nothing in this Article shall invalidate any law — (a) in force before the commencement of this Constitution which authorises the arrest and detention of any person in the interests of public safety, peace and good order; or (b) relating to the misuse of drugs or intoxicating substances which authorises the arrest and detention of any person for the purpose of treatment and rehabilitation, by reason of such law being inconsistent with clauses (3) and (4), and, in particular, nothing in this Article shall affect the validity or operation of any such law before 10th March 1978. **Equal protection** 12.—(1) All persons are equal before the law and entitled to the equal protection of the law. (2) Except as expressly authorised by this Constitution, there shall be no discrimination against citizens of Singapore on the ground only of religion, race, descent or place of birth in any law or in the appointment to any office or employment under a public authority or in the administration of any law relating to the acquisition, holding or disposition of property or the establishing or carrying on of any trade, business, profession, vocation or employment. (3) This Article does not invalidate or prohibit — (a) any provision regulating personal law; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(b) any provision or practice restricting office or employment connected with the affairs of any religion, or of an institution managed by a group professing any religion, to persons professing that religion. **Freedom of speech, assembly and association** 14.—(1) Subject to clauses (2) and (3) — (a) every citizen of Singapore has the right to freedom of speech and expression; (b) all citizens of Singapore have the right to assemble peaceably and without arms; and (c) all citizens of Singapore have the right to form associations. (2) Parliament may by law impose — (a) on the rights conferred by clause (1)(a), such restrictions as it considers necessary or expedient in the interest of the security of Singapore or any part thereof, friendly relations with other countries, public order or morality and restrictions designed to protect the privileges of Parliament or to provide against contempt of court, defamation or incitement to any offence; (b) on the right conferred by clause (1)(b), such restrictions as it considers necessary or expedient in the interest of the security of Singapore or any part thereof or public order; and (c) on the right conferred by clause (1)(c), such restrictions as it considers necessary or expedient in the interest of the security of Singapore or any part thereof, public order or morality. (3) Restrictions on the right to form associations conferred by clause (1) (c) may also be imposed by any law relating to labour or education.
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	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	
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.	

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.	
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;	CRIMINAL PROCEDURE CODE (CHAPTER 68) **Power to access computer** 39.—(1) A police officer or an authorised person investigating an arrestable offence may, at any time — (a) access, inspect and check the operation in or from Singapore of a computer (whether in Singapore or elsewhere) that the police officer or authorised person has reasonable cause to suspect is or has been used in connection with, or contains or contained evidence relating to, the arrestable offence; (b) use any such computer in or from Singapore, or cause any such computer to be used in or from Singapore — (i) to search any data contained in or available to such computer; and (ii) to make a copy of any such data; (c) prevent any other person from gaining access to, or using, any such computer (including by changing any username, password or other authentication information required to gain access to the computer); or (d) order any person — (i) to stop accessing or using or to not access or use any such computer; or (ii) to access or use any such computer only under such conditions as the police officer or authorised person may specify.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	[Act 19 of 2018 wef 17/09/2018] (2) The police officer or authorised person may also order any of the following persons to provide any assistance mentioned in subsection (2A): (a) any person whom the police officer or authorised person reasonably suspects of using, or of having used, the computer in connection with the arrestable offence; (b) any person having charge of, or otherwise concerned with the operation of, the computer; (c) any person whom the police officer or authorised person reasonably believes has knowledge of or access to any username, password or other authentication information required to gain access to the computer. [Act 19 of 2018 wef 17/09/2018] (2A) For the purposes of subsection (2), the types of assistance are as follows: (a) assistance to gain access to the computer (including assistance through the provision of any username, password or other authentication information required to gain access to the computer); (b) assistance to prevent a person (other than the police officer or authorised person) from gaining access to, or using, the computer, including assistance in changing any username, password or other authentication information required to gain access to the computer. [Act 19 of 2018 wef 17/09/2018] (2B) Without limiting subsection (1), where the police officer or authorised person knows that the computer mentioned in that subsection is located outside Singapore, or does not know whether that computer is located in or outside Singapore, the police officer or authorised person — (a) may exercise the powers under subsection (1) in relation to that computer, or any data contained in or available to that computer, if — (i) the owner of that computer consents to the exercise of those powers; or (ii) the police officer or authorised person obtains access to that computer through the exercise of any power of investigation under any written law, such as in any of the following circumstances: (A) the access is obtained with the assistance mentioned in subsection (2A)(a) provided under subsection (2) by a person having charge of, or otherwise concerned with the operation of, that computer; (B) the access is obtained through an active connection with, or through any username, password or other authentication information stored in, another

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	computer, which has been seized under section 35 and accessed under subsection (1); (C) the access is obtained through any username, password or other authentication information contained in any document seized under section 35; (D) the access is obtained through any username, password or other authentication information provided in any statement made by any person examined under section 22; and (b) may exercise the powers under subsection (1)(b) in relation to any data contained in or available to that computer, if the owner of that data consents to the exercise of those powers. [Act 19 of 2018 wef 17/09/2018] (3) Any person who obstructs the lawful exercise by a police officer or an authorised person of any power under subsection (1)(a), (b) or (c), or who fails to comply with any order of the police officer or authorised person under subsection (1)(d) or (2), shall be guilty of an offence and shall be liable on conviction — (a) in any case where the person is a body corporate, a limited liability partnership, a partnership or an unincorporated association — to a fine not exceeding $10,000; or (b) in any other case — to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 6 months or to both. [Act 19 of 2018 wef 17/09/2018] (4) An offence under subsection (3) shall be an arrestable offence. (5) A person who had acted in good faith under subsection (1) or in compliance with a requirement under subsection (1)(d) or (2) shall not be liable in any criminal or civil proceedings for any loss or damage resulting from the act. [Act 19 of 2018 wef 17/09/2018] (6) In this section and section 40 — "authorised person" means — (a) a forensic specialist appointed under section 65A of the Police Force Act (Cap. 235), or any other person, who is authorised in writing by the Commissioner of Police for the purposes of this section or section 40 or both; or (b) any officer of a prescribed law enforcement agency who is authorised in writing, by the head of that law enforcement agency, for the purposes of this section or section 40 or both;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	"prescribed law enforcement agency" means a law enforcement agency prescribed, by order in the Gazette, by the Minister charged with the responsibility for that law enforcement agency. [Act 19 of 2018 wef 17/09/2018] **Power to access decryption information** 40.—(1) For the purposes of investigating an arrestable offence, the Public Prosecutor may by order authorise a police officer or an authorised person to exercise, in addition to the powers under section 39, all or any of the powers under this section. (2) The police officer or authorised person referred to in subsection (1) shall be entitled to — (a) access any information, code or technology which has the capability of retransforming or unscrambling encrypted data into readable and comprehensible format or text for the purposes of investigating the arrestable offence; (b) require — (i) any person whom he reasonably suspects of using a computer in connection with an arrestable offence or of having used it in this way; or (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); and (c) require any person whom he reasonably suspects to be in possession of any decryption information to grant him access to such decryption information as may be necessary to decrypt any data required for the purposes of investigating the arrestable offence. (3) Any person who obstructs the lawful exercise by a police officer or an authorised person of the powers under subsection (2)(a) or who fails to comply with any requirement of the police officer or authorised person under subsection (2)(b) or (c) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both. (4) Where a person is convicted of an offence under subsection (3) and it is shown that the encrypted data contains evidence relevant to the planning, preparation or commission of a specified serious offence, he shall, in lieu of the punishment prescribed under subsection (3) —

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) be liable to be punished with the same punishment prescribed for that specified serious offence, except that the punishment imposed shall not exceed a fine of $50,000 or imprisonment for a term not exceeding 10 years or both; or (b) be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both where the specified serious offence is punishable on conviction with death or imprisonment for life. (5) For the purposes of subsection (4) but subject to subsection (6), "specified serious offence" means an offence under any of the following written laws: (a) any written law which provides for any offence involving the causing of death or bodily harm; (b) any written law relating to actions or the threat of actions prejudicial to national security; (c) any written law relating to radiological or biological weapons; (d) the Arms and Explosives Act (Cap. 13); (e) the Chemical Weapons (Prohibition) Act (Cap. 37B); (f) the Corrosive and Explosive Substances and Offensive Weapons Act (Cap. 65); (g) the Hijacking of Aircraft and Protection of Aircraft and International Airports Act (Cap. 124); (h) the Kidnapping Act (Cap. 151); (i) the Maritime Offences Act (Cap. 170B); (j) the Official Secrets Act (Cap. 213); (k) the Infrastructure Protection Act 2017; [Act 41 of 2017 wef 18/12/2018] (l) the Statutory Bodies and Government Companies (Protection of Secrecy) Act (Cap. 319); (m) the Strategic Goods (Control) Act (Cap. 300); (n) the Terrorism (Suppression of Financing) Act (Cap. 325); (o) the United Nations (Anti-Terrorism Measures) Regulations (Cap. 339, Rg 1); and (p) such other written law as the Minister may, by order published in the Gazette, specify. (6) No offence shall be a specified serious offence for the purposes of subsection (4) unless the maximum punishment prescribed for that offence, whether for a first or subsequent conviction, is — (a) imprisonment for a term of 5 years or more; (b) imprisonment for life; or

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(c) death. (7) In proceedings against any person for an offence under this section, if it is shown that that person was in possession of any decryption information at any time before the time of the request for access to such information, that person shall be presumed for the purposes of those proceedings to have continued to be in possession of that decryption information at all subsequent times, unless it is shown that the decryption information — (a) was not in his possession at the time the request was made; and (b) continued not to be in his possession after the request was made. (8) A person who had acted in good faith or in compliance with a requirement under subsection (2) shall not be liable in any criminal or civil proceedings for any loss or damage resulting from the act. (9) In this section — "data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer; "decryption information" means information, code or technology or part thereof that enables or facilitates the retransformation or unscrambling of 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 the original data before it has been transformed or scrambled to an unreadable or incomprehensible format.
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,	

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.	
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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
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.	PART III MISCELLANEOUS AND GENERAL **Territorial scope of offences under this Act** 11.—(1) Subject to subsection (3), the provisions of this Act shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within Singapore. [Act 22 of 2017 wef 01/06/2017] (2) Where an offence under this Act is committed by any person in any place outside Singapore, he may be dealt with as if the offence had been committed within Singapore. (3) For the purposes of this section, this Act applies if — (a) for the offence in question, the accused was in Singapore at the material time; (b) for the offence in question (being one under section 3, 4, 5, 6, 7 or 8), the computer, program or data was in Singapore at the material time; or (c) the offence causes, or creates a significant risk of, serious harm in Singapore. [Act 22 of 2017 wef 01/06/2017] (4) In subsection (3)(c), "serious harm in Singapore" means — (a) illness, injury or death of individuals in Singapore; (b) a disruption of, or a serious diminution of public confidence in, the provision of any essential service in Singapore; [Act 9 of 2018 wef 31/08/2018] (c) a disruption of, or a serious diminution of public confidence in, the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board; or (d) damage to the national security, defence or foreign relations of Singapore. Example 1.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the provision of an essential service:

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(a) publication to the public of the medical records of patients of a hospital in Singapore; (b) providing to the public access to the account numbers of customers of a bank in Singapore. Example 2.— The following are examples of acts that seriously diminish or create a significant risk of seriously diminishing public confidence in the performance of any duty or function of, or the exercise of any power by, the Government, an Organ of State, a statutory board, or a part of the Government, an Organ of State or a statutory board: (a) providing to the public access to confidential documents belonging to a ministry of the Government; (b) publication to the public of the access codes for a computer belonging to a statutory board. [Act 22 of 2017 wef 01/06/2017] (5) For the purposes of subsection (3)(c), it is immaterial whether the offence that causes the serious harm in Singapore — (a) causes such harm directly; or (b) is the only or main cause of the harm. [Act 22 of 2017 wef 01/06/2017] (5A) In subsection (4)(b), "essential service" means any of the following services: (a) services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure; (b) emergency services such as police, civil defence or health services. [Act 9 of 2018 wef 31/08/2018] (6) In subsection (4)(c), "statutory board" means a body corporate or unincorporate established by or under any public Act to perform or discharge a public function. [Act 22 of 2017 wef 01/06/2017] […] **Jurisdiction of Courts** 12. A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this Act and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Chapter III – International co-operation	
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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;	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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, 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; 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:	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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