Nepal

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 01/04/2020

[reference to the provisions of the Budapest Convention]

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

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

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	Electronic Transactions Act, 2063 (2008) - ETA Art. 2 (g): "Computer System" means a device or a group of devices, containing all computer programmes including input and output support devices, electronic instructions, input and output data that performs logical, arithmetic, data storage and retrieval, communication including controlling functions. *[Definition of largely consistent with the BC, but less technology neutral.]* Art. 2 (d): "Computer" means an electro-magnetic, optical or other high-speed data processing device or system, which performs logical, arithmetic and memory functions by manipulating electro-magnetic or optical impulses, and also includes all acts of input, output, processing, storage and computer software or communication facilities which are connected or related to the computer in any computer system or computer network. Art. 2 (f): "Computer Network" means an interrelationship between two or more than two computers having interconnection with each other or in contact of communication. Art. 2 (h): "Computer Resource" means a computer, computer system, computer network, data, computer database or software. *[The definitions of computer system, computer network and computer have overlapping meanings. At the same time any device, system or network could be referred to as a computer resource, which seems to be a generic reference to all the previous.]*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Art. 2 (e): "Computer Database" means an information, knowledge and concept or presentation of instructions, which are being prepared or have already been prepared in word, image, voice or audio visual form in a formalized manner or which have been produced by a computer, computer system or computer network, with a view to use in a computer, computer system or computer network. Art. 2 (k): "Data" means the presentation of information, knowledge, fact and concept or instructions in any form, which are kept in a formalized manner in a computer system or computer network and is intended for processing the same, or processed or stored in a computer memory. *[Definition is largely consistent with the Budapest Convention]* Art. 2 (c): "Originator" means a person who generates, stores or transmits electronic records, and this term also includes a person who causes any other person to carry out such functions: Provided that it shall not include an intermediary. *[The ETA uses the term 'originator' which does not cover the definition of a 'service provider' as defined in the Budapest Convention.]*
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.	Art. 45: Unauthorized Access in Computer Materials: If any person with an intention to have access in any programme, information or data of any computer, uses such a computer without authorization of the owner of or the person responsible for such a computer or even in the case of authorization, performs any act with an intention to have access in any programme, information or data contrary to from such authorization, such a person shall be liable to the punishment with the fine not exceeding Two Hundred Thousand Rupees or with imprisonment not exceeding three years or with both depending on the seriousness of the offence. *[Inconsistent with the BC as it is missing the element of accessing "whole or any*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	part of a computer system", thus potentially having an under-criminalizing effect.]
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.	
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.	Art. 46: Damage to any Computer and Information System: If any person knowingly and with a mala fide intention to cause wrongful loss or damage to any institution destroys, damages, deletes, alters, disrupts any information of any computer source by any means or diminishes value and utility of such information or affects it injuriously or causes any person to carry out such an act, such a person shall be liable to the punishment with the fine not exceeding two thousand Rupees and with imprisonment not exceeding three years or with both. *[The ETA provision is to certain extent consistent with the BC. Nevertheless, the intention is formulated very strict: 'a mala fide intention to cause wrongful loss or damage to any institution'.]*
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	Art. 44 ETA: To Pirate, Destroy or Alter computer source code: When computer source code is required to be kept as it is position for the time being the prevailing law, if any person, knowingly or with malafide intention, pirates, destroys, alters computer sources code to be used for any computer, computer programme, computer system or computer network or cause, other to do so, he/she shall be liable to the punishment with imprisonment not exceeding three years or with a fine not exceeding two hundred thousand Rupees or with both. Explanation: For the purpose of this section "computer source code" means the listing of programmes, computer command, computer design and layout and programme analysis of the computer resource in any form. *[The ETA provision is to some extent consistent with the Budapest Convention.]*
Article 6 – Misuse of devices	

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.	
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,	Art. 49: To inform False statement: If any person with an intention to obtain a license from Certifying Authority under this Act or with any other intention either to Controller or with an intention to obtain Digital Signature Certificate or with any other intention conceals statement knowingly or lies any statement to be submitted to the Certifying Authority any false statements shall be liable to the

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.	punishment with a fine not exceeding One Hundred Thousands rupees or with an imprisonment not exceeding two years or with both. *[Not in line with the range and scope of the BC and has other specific objectives related to the ratio legis of the ETA.]* Art. 50: Submission or Display of False License or Certificates: (1) If any person who works as a Certifying Authority without a license issued by the Controller under this Act, shall be liable to the punishment with a fine not exceeding one hundred thousand Rupees or with an imprisonment not exceeding two years or with both, depending on seriousness of the offence. (2) Any person without obtaining a license from the Certifying Authority publishes a fake license or false statement in regard to license or provides to any person by any other means, shall be liable to the punishment not exceeding one hundred thousand Rupees in the case where the act referred to in Sub-section (1) has not been accomplished by such a person. (3) If any person publishes or otherwise makes available a certificate to any other person by any means knowingly that a certificate is not issued by the Certifying Authority referred to in such a certificate or the subscriber listed in such certificate has not accepted the certificate or such a certificate is already suspended or revoked, shall be liable to the punishment with a fine not exceeding one hundred thousand Rupees or with an imprisonment not exceeding two years or with both. Provided that, if such a certificate suspended or revoked is published or provided for the purpose of verification of the Digital Signature before it was suspended or revoked, it shall not be deemed to have been committed an offence under this Sub-section. *[Too restrictive and narrows down the criminalization of (computer related) forgery to the situation that is related to a 'false certificate', a 'fake license' or a 'false statement' with an intention to mislead the certifying authority.* *ETA has no real substantive law provision that meets the requirements and scope of article 7 Budapest Convention.]* Part-4 Chapter-1 On Forged Document (Forgery), Numbers 1 to 18 GC

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	[This domestic provision of the General Code – GC, is about the forgery of documents, not computer data.]
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.	Art. 52 ETA: To commit computer fraud: If any person, with an intention to commit any fraud or any other illegal act, creates, publishes or otherwise provides digital signature certificate or acquires benefit from the payment of any bill, balance amount of any one's account, any inventory or ATM card in connivance of or otherwise by committing any fraud, amount of the financial benefit so acquired shall be recovered from the offender and be given to the person concerned and such an offender shall be liable to the punishment with a fine not exceeding one hundred thousand Rupees or with an imprisonment not exceeding two years or with both. *[Article not consistent with the Budapest Convention.]* Part 4, Chapter-3 Cheating, Numbers 1 to 8 GC *[This provision does not meet the specific requirements of 'computer related fraud' of the BC.]*
Title 3 – Content-related offences	
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography for the purpose of its distribution through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium.	Art. 47 ETA: Publication of illegal materials in electronic form: (1) If any person publishes or displays any material in the electronic media including computer, internet which are prohibited to publish or display by the prevailing law or which may be contrary to the public morality or decent behavior or any types of materials which may spread hate or jealousy against anyone or which may jeopardize the harmonious relations subsisting among the peoples of various castes, tribes and communities shall be liable to the punishment with the fine not exceeding One Hundred Thousand Rupees or with the imprisonment not exceeding five years or with both. (2) If any person commit an offence referred to in Sub-section (1) time to time he/she shall be liable to the punishment for each time with one and one half percent of the punishment of the previous punishment.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	*[The provision is not specifically designed as an offence related to child pornography, but can be generally applied to prosecute in such cases. However,it is not consistent with the Budapest Convention.]* The Children's Act, 2048 (1992), 2049/2/7 (May 20, 1992 A.D.) - CA Art. 2 -Definitions: Unless the subject or context otherwise requires, in this Act, (a) "Child" means a minor not having completed the age of sixteen years. (…) *[The term "minor" includes all persons under 16 years of age, which is consistent with the Budapest Convention.]* Art. 16 - Children not to be involved in immoral profession: (1) No person shall involve or use a Child in immoral profession. (2) No photograph of a Child shall be taken or allowed to be taken, nor such photograph shall be distributed or exhibited for the purpose of engaging a Child in immoral profession. (3) No publication, exhibition or distribution of photograph or personal events or descriptions of a Child tarnishing the character of such Child shall be made. (4) No Child shall be involved in the sale or distribution or smuggling of intoxicating substances, narcotic drugs or any other drugs. *[The Children's Act does criminalize any involvement of a child in an immoral profession. It does not focus on child pornography and does not meet the requirements of art. 9.1 and 9.2 BC, even though art. 16 CA could cover some of the actions focused on in art 9 BC.]* Art. 53 - Punishment: (…) (4) Whoever commits any offence in contravention to sub- section (1), (2) or (3) of Section 16 or abets others to commit such offence or attempts to do so, he shall be liable to a punishment with a fine up to ten thousand rupees or with imprisonment for a term which may extend to one year or with both and the photographs taken with an aim to engage the Child in an immoral profession and all the publications printed with an aim to publish may be seized by the order of the Court.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	(5) The person engaging a Child in the business in contravention to sub-section (4) of Section 16 shall be punished with imprisonment for a term which may extend to five years in addition to the punishment to be imposed pursuant to existing laws. (6) In case character of a Child is hurt or adverse effect is caused in his health or his physical organ is damaged due to the reason that any person has caused the Child to engage in any prohibited act pursuant to Section 16, ... the officer hearing the case may cause to pay a reasonable amount of compensation in proportion to such damage to the Child from such person in addition to the punishment to be imposed pursuant to sub-section (1) or (4). *[The offences related to child pornography are also under-criminalized under the CA:* *- No definition of 'immoral profession'* *- The taking, exhibition or distribution of a photograph is only criminalized when it is done 'for the purpose of engaging a Child in immoral profession';* *- The law requires 'tarnishing the character of such child'.]*
Title 4 – Offences related to infringements of copyright and related rights	
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral 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	The Copyright Act, 2059 (2002) – CRA – in particular: Chapter-6 Infringement of Protected Right and Punishment 25. Infringement of protected right : (1) Any one who carries out the following act shall be considered to have infringed the right protected under this Act:- (a) To reproduce copies of a work or sound recording and sell and distribute them or publicly communicate or rent them with

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.	commercial or any other motive with or without deriving economic benefits without authorization of the author or the copyright owner or by infringing the terms contained in the agreement or license notwithstanding that such authorization has been obtained, (b) To do advertisement or publicize by copying a work belonging to another person with a motive of taking advantage of the reputation gained by that work, (c) To make work of another subject or nature by changing the form and language of a work belonging to another person with a motive of deriving economic benefit, (d) To make an attempt to take benefit by adapting any work directly or indirectly with intention of making the viewer, listener or reader believe it to be another work through advertisement or by any other means, (e) To import, produce or rent any equipment or device prepared with intention of circumventing any device designed to discourage the unauthorized reproduction, (f) To produce or import, with intent to sell, any equipment facilitating unauthorized reception of a program broadcast by encrypting it in a code language, (g) To import, sell, distribute and use a mechanical device prepared with a sole object of infringing the copyright, except those mentioned in Clauses (e) and (f). (2) No one shall, with knowledge of publication of any work or sound recording or where there is adequate ground to believe it, sell and distribute and rent copies of work or sound recording so published, in contravention of sub- section (1). 26. Restriction on the importation of unauthorized copies: Importation of copies of work or sound recording, either made in a foreign country or sourced otherwise, into Nepal for business purpose shall not be permitted if preparation of such copies would be considered illegal if they were prepared in Nepal.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	27. Punishment on infringement of protected right : (1) In cases where any person infringes Section 25, such a person shall be punished with a fine of a sum from ten thousand to one hundred thousand rupees or with imprisonment for a term not exceeding six months or both and with a fine of a sum from twenty thousand to two hundred thousand rupees or with imprisonment for a term not exceeding one year or with both for each instance from the second time. The materials so published or reproduced or distributed or devices used to reproduce such materials shall be seized. (2) Compensation for the loss caused to the copyright owner by the infringer of the protected right shall also be realized and provided to the copyright owner. 28. Punishment for importation of unauthorized copy : In cases where any person imports unauthorized copies of any work in violation of Section 26, such a person shall be punished with a fine of a sum from ten thousand to one hundred thousand rupees according to the gravity of the offense, and such copies shall be seized; and compensation for the loss caused to the copyright owner from such importation shall also be realized from the importer and provided to the copyright owner. 29. Other punishment : In cases where any person infringes any other matter contained in this Act or the Rules framed under this Act, such a person shall be punished with a fine of a sum from five thousand to fifty thousand rupees according to the gravity of the offense. *[The CRA seems sufficiently consistent with the Budapest Convention.]*
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.	Electronic Transactions Act, 2063 (2008) - ETA Art. 53: Abetment to commit computer related offence: A person who abets other to commit an offence relating to computer under this Act or who attempts or is involved in the conspiracy to commit such an offence shall be liable to the punishment with a fine not exceeding fifty thousand Rupees or with imprisonment not exceeding six months or with both, depending on the degree of the offence.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Art. 54: Punishment to the Accomplice: A person who assists others to commit any offence under this Act or acts as accomplice, by any means shall be liable to one half of the punishment for which the principal is liable.. *[Largely consistent with the Budapest Convention.]*
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.	Art. 57: Offences Committed by a corporate body: (1) If any act is done by a corporate body which deems an offence under this Act, such an offence shall be deemed to have been committed by a person who was responsible as chief for the operation of the corporate body at the time of committing such an offence. Provided that, if the person who was responsible as a chief for the operation of such a corporate body proves that such an offence was committed without his/her knowledge or that he/she exercised all reasonable efforts to prevent such an offence, he/she shall not be liable to the guilty. *[Section (1) not consistent with the Budapest Convention.]* (2) Notwithstanding anything contained in Sub-section (1), if it is proved that any offence under this Act committed by a corporate body with the consent or in knowledge or by the reason of negligence of a director, manager, secretary or any other responsible person of such corporate body, such an offence shall be deemed to have been committed by such a corporate body and by a director, manager, secretary or other responsible person of such a corporate body. *[Section (2) of article 57 is largely consistent with art. 12.2 Budapest Convention.]*
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.	Art. 56: Confiscation: Any computer, computer system, floppy, compact disks, tape drivers, softwares or any other accessory devices used to commit any act deemed to be an offence relating to computer under this Act shall be liable to confiscation. Art. 58: Other Punishment: If any violation of this Act or Rules framed hereunder has been committed, for which no penalty has been separately provided, such a violator shall be liable to the punishment with a fine not exceeding fifty thousand Rupees, or with an imprisonment not exceeding six months or with both.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Art. 59: No Hindrance to Punish Under the Laws prevailing: If any act deemed to be an offence under this Act shall also be deemed to be another offence under the laws prevailing, it shall not be deemed to have been hindered by this Act to file a separate case and punish accordingly. *[The domestic legislation is largely consistent with art. 13.1 Budapest Convention. There is no consistency however with art. 13.2 Budapest Convention]*
Section 2 – Procedural law	
Article 14 – Scope of procedural provisions 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings. 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to: a the criminal offences established in accordance with Articles 2 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,	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.	
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; b make and retain a copy of those computer data;	.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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 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.	The Nepal Communications Act 2053 (1997) Art. 19: Special Powers of His Majesty's Government: (1) In case it requires to stop the transmission of information or to control transmission system due to the state of emergency or national security, His Majesty's Government may carry out the following acts: (a) To take temporarily the Telecommunications Line and the Telecommunications System installed, operated or supervised by the Licensee under its possession, (b) To order to tape the information, to trace the transmitter of the information or to stop such information related to any specific subject, person or community. *[The domestic provision is not consistent with the BC. It only applies 'due to the state of emergency or national security'. Further, in relation with 'interception of content data', the provision only refers to 'order to tape the information'. There is no legal framework, containing conditions and safeguards, to ensure a balanced empowerment of 'His Majesty's Government'.]*

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Art. 19 TA: Special Powers of His Majesty's Government: Art. 19: Special Powers of His Majesty's Government: (1) In case it requires to stop the transmission of information or to control transmission system due to the state of emergency or national security, His Majesty's Government may carry out the following acts: (a) To take temporarily the Telecommunications Line and the Telecommunications System installed, operated or supervised by the Licensee under its possession, (b) To order to tape the information, to trace the transmitter of the information or to stop such information related to any specific subject, person or community. *[The domestic provision is not consistent with the BC. It only applies 'due to the state of emergency or national security'. Further, in relation with 'interception of content data', the provision only refers to 'order to tape the information'. There is no legal framework, containing conditions and safeguards, to ensure a balanced empowerment of 'His Majesty's Government'.]*
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.	Electronic Transactions Act, 2063 (2008) - ETA Art. 55 ETA: Punishment in an offence committed outside Nepal: Notwithstanding anything contained in the prevailing laws, if any person commits any act which constitutes an offence under this Act and which involves the computer, computer system or computer network system located in Nepal, even though such an act is committed while residing outside Nepal, a case may be filed against such a person and shall be punished accordingly. Art. 1 (3) ETA: This Act shall extend throughout Nepal and shall also apply to any person residing anywhere by committing an offence in contravention to this Act.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 55 and 1 (3 - first part) is consistent with article 22.1.a Budapest Convention as far as it establishes jurisdiction for crimes committed on the territory of Nepal.* *In the second part of article 1 (3), the ETA seems to establish some sort of universal jurisdiction against any person who committed an offence in contravention with the ETA anywhere. The text of article 1(3) does not expressly require a territorial link and does not prescribe a 'nationality' requirement.]*
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	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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, 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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; 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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