Lao People's Democratic Republic

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 24 April 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	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 3 - Definitions The terms used in this law have the following meaning: 1. **Crime** means any offence prescribed in the Penal Code and any other law prescribed criminal penalty; 2. **Computer System** means a piece of electronic equipment or sets of electronic equipment units is integrated together, for which contains an ordering, sets of ordering and other related process to enable the electronic equipments to perform the duty of processing data automatically in a computer or any interconnected computers through computer network or internet system; 3. **Server System** means a service system providing through the Computer System including Database Server, Web Server, Mail Server, File Server and other related components; 4. **Computer's data and information** means data, message, program or database system, personal data and information, computer traffic data in form of data processing and enabling computer to perform a function; 5. **Database System** means a storage data system in form of electronic mean that being able to manage, modify and use; 6. **Personal Data and Information** means any data and information directly or indirectly relating and identifying individual action of person, legal entity and organization; 7. **Computer Traffic Data** means data related to communication through computer system-based developed by a computer system as a part of communication chain showing sender, source of origin, intermediary, route, destination, time, date as well as size and duration of communication, type of service and other service concerned relating to computer system communication;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	8. **Service Provider** means a person providing of communication data and information through computer system and/or a person providing of computer data storage; 9. **Automatically Data Processing** means a process of calculating and developing data in any computer system by a computer program; 10. **Program** means an ordering system, computer network, computer's data and information; 11. **Virus** means any specifically developed program for wide spreading virus, damaging and destroying computer system, computer network, computer's data and information; 12. **Malicious Code** means any developed set of ordering for destroying computer system or hacking computer's data and information; 13. **Fishing Website** means any new creating website containing the same characters and components similar to the original website in order to deceive for obtaining consumer information; 14. **Vulnerability** means a weakness of any software or program which is not be accomplished or updated allowing an attacker to use for destroying computer system, hacking or changing data, information and others in computer system; 15. **Consumer Information** means any information on consumer's address such as postal address, electronic address, geographical address, internet protocol, telephone number and other related code applying into any computer; 16. **Specific Access Prevention Measure** means an applying of any specific tool and/or program into any computer for prevention and combating others from unauthorized computer access; 17. **Online Social Media** means an internet system disseminating and providing data and information to public by means of computer equipments and communication devices; 18. **Animation** means any created image moving as live action which can be visible through an electronic device such as cartoon movies.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 10. Unauthorized Computer Access Unauthorized computer access is an offence applying an electronic equipment or device to access any computer having specific computer access prevention measure or steal any commercial, financial data and information as well as secret confidence, other related information of person, legal entity and organization. Telecommunication Law 2001 Article 29. Penal Measures A person who has violated the provisions of the Law on Telecommunications as described below shall be subject to penal punishment: 1. Use of communications to defeat national stability, peace, [or the] socio-economic or cultural development [of the country]; 2. Use of telecommunication systems to defame persons or organisations; 3. Tampering with frequency waves, or using any telecommunication equipment, [or] telecommunication network of their own to connect into frequency waves or any telecommunication equipment or network operated by others to obstruct, interrupt, encroach [on], destroy, modify, erase, tap [into], intercept, steal or retrieve other person's data [and] information; 4. Destruction of public or individual14 telecommunication systems and equipment; 5. Illegal importation of telecommunication equipment; 6. Abuse of position, abuse of power, giving and receiving bribes, falsifying documents, improper issuance of documents relating to the establishment and provision of telecommunication service; 7. Other criminal offences related to telecommunication activities. Terminal Equipment refers to telecommunication equipment used by service users, such as wired or wireless telephone sets, facsimile units, computer units, accessories and internal wires which are the property of the service users; 7. Telecommunication Network refers to the central system of the telecommunication infrastructure which includes wired and wireless systems or systems integrating both [wired and wireless components], including equipment incorporated into telecommunication services;

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 12. Unauthorized Interception of Computer's Data and Information Unauthorized Interception of Computer's Data and Information is an offence of interception of Computer's Data and Information by mean of applying any electronic equipment or device while the receiver is receiving, or the sender is sending, data and information via 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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 17. Destroying Computer's Data and Information Destroying Computer's Data and Information is an offence of deleting, editing and/or modifying of computer's data and information or data and information in computer system in order to cause data and information in computer system being damage and different from original aspects.
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	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 15. Computer System Interference Computer System Interference are offences in the actions of following: 1. Using of comport program, virus or other tools to interrupt or destroy the performance of computing; 2. Sending of computer system, data and information or electronic mail or message with concealing of address, source of sender to disturb and/or destroy the performance of computing.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 6 – Misuse of devices 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of: i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 9. Disclosing of Specific Computer Access Prevention Measure Disclosing of specific computer access prevention measure is an offence taking specific computer access prevention measure to reveal without any authorization causing damage to state, person, legal entity, organization and society. Article 18. Operating Business of Tools and Equipments for Cyber Crime Operating Business of Tools and Equipments for Cyber Crime is an offence of developing if any new specific program, producing, importing, possessing, selling and buying, distributing, advertising, disseminating or distributing the tools and equipment such as computer program or designing of computer's data and information for committing any cyber crime
Title 2 – Computer-related offences	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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, 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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 16. Computer's Data and Information Forgery Computer's Data and Information Forgery is an offence of using the computer, computer system and electronic equipment or device by means of action of following: 1. Intentionally inputting and changing data and information, forgery of electronic address or deleting of data and information in any computer consequently causing outcome of changing from the original data and information; 2. Inputting and changing data and information of financial and commercial transaction, secrete confidence as well as other data and information of person, legal entity, organization without any authorization; 3. Developing of fake website to mislead, deceive other person using computer system or internet to input data and information of bank account, credit card codes, internet usage card codes as well as the other data and information concerned. Art. 150 (general meaning of forgery) of the Penal Law of the Lao People's Democratic Republic. Any person forging documents, signatures, or seals, or deleting or adding words to documents shall be punished by three months to two years of imprisonment and shall be fined from 200,000 Kip to 2,000,000 Kip. Any person knowingly using forged documents shall be punished by three months to two years of imprisonment and shall be fined from 200,000 Kip to 2,000,000 Kip. Where the forgery or use of forged documents causes substantial damage, the offender shall be punished by two to five years of imprisonment and shall be fined from 500,000 Kip to 10,000,000 Kip. Article 106. Forgery or Destruction of Election Documents Any person forging or destroying election documents, or forging or destroying ballots or the results of an election to the National Assembly, shall be punished by one to two years of imprisonment and shall be fined from 200,000 Kip to 2,000,000 Kip.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Article 161. Forgery of Documents or Use of Forged Documents Any person forging documents, signatures, or seals, or deleting or adding words to documents shall be punished by three months to two years of imprisonment and shall be fined from 200,000 Kip to 2,000,000 Kip. Any person knowingly using forged documents shall be punished by three months to two years of imprisonment and shall be fined from 200,000 Kip to 2,000,000 Kip. Where the forgery or use of forged documents causes substantial damage, the offender shall be punished by two to five years of imprisonment and shall be fined from 500,000 Kip to 10,000,000 Kip.
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.	
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;	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 14. Dissemination of Pornography Pornography is data and information containing of context clearly appearing in physical aspects such as picture and image, animation, audio, video relating to sexual organs and sexual activities of human.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Dissemination of Pornography is an offence of selling, buying, distributing, transferring, introducing and disseminating of above prescribed in this Article. Art. 125 (general meaning of pornography) of the Penal Law of the Lao People's Democratic Republic. Any person who, in the presence of members of the public or in any public place, engages in an act of sexual intercourse or exposes his or her sexual organs shall be punished by three months to one year of imprisonment or re-education without deprivation of liberty and shall be fined from 50,000 Kip to 200,000 Kip. For Art. 9(/a-c) - Art. 127 of the Penal Law of the Lao People's Democratic Republic. Any person engaging in the widespread production, distribution, or dissemination of pornographic items, magazines, pictures, video cassettes and other materials contrary to fine traditions shall be punished by three months to one year of imprisonment and shall be fined from 200,000 Kip to 5,000,000 Kip. Article 138. Dissemination of Pornographic Objects and Objects Contrary to Fine Traditions Any person engaging in the widespread production, distribution, or dissemination of pornographic items, magazines, pictures, video cassettes and other materials contrary to fine traditions shall be punished by three months to one year of imprisonment and shall be fined from 200,000 Kip to 5,000,000 Kip.
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	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 20155 Article 11. Unauthorized Editing Picture, Animation, Audio and Video Unauthorized Editing Picture, Animation, Audio and Video is an offence of editing picture or image, adding or modifying the original version by mean of electronic

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	process or other means in order to disseminate the outcome through computer system causing damage to state, person, legal entity and organization concerned.
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.	Lao People's Democratic Republic Penal Law (amended) of 9 December 2005 Article 13. Preparation to Commit Offences "Preparation to commit an offence" refers to the preparation of materials, conditions or other factors in order to commit an intentional offence. Such preparation to commit an offence shall only be charged or punished if deemed dangerous for society, as provided in the specific part of this law. Preparation to commit offences shall be punished according to the articles prescribing penalties for the offence itself. Article 14. Attempts to Commit Offences "Attempt to commit an offence" refers to the taking of intentional acts which are components of an offence but where the offence was not completed because of circumstances outside the control of the offender, making such acts not successful.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Such attempts to commit an offence shall only be charged or punished if deemed dangerous for society, as provided in the specific part of this law. Attempts to commit an offence shall be punished according to the articles prescribing penalties for the offence itself. For Art.11(2)- Art. 13 (general meaning of attempt) of the Penal Law of the Lao People's Democratic Republic. "Attempt to commit an offence" refers to the taking of intentional acts which are components of an offence but where the offence was not completed because of circumstances outside the control of the offender making such acts not successful. Such attempts to commit an offence shall only be charged or punished if deemed dangerous for society, as provided in the specific part of this law. Attempts to commit an offence shall be punished according to the articles prescribing penalties for the offence itself.
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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 6. Scope of the law enforcement This law applies to person, legal entity and organizations, both domestic and foreign country, living and researching and operating computer system and computer's data and information in the Lao PDR.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 57. Measures against Violators Any person, legal entity or organization violating a statute of this law primarily defined prohibitions shall undergo warning, re-education, discipline and fine measures, compensation of incurred civil damage or criminal sanctions in accordance with the case severity level of violation. Article 58. Re-education measures Any person, legal entity or organization violating a statute of this law regarding as the first violation and incurring minor damages shall be undergone warning and re-education measures. Article 59. Disciplinary Measures Any staff personnel, officials concerned violating of this law which is not a criminal offence shall be subjected to disciplinary basing on case by case of violating as following: 1 - Denouncing, warning of violation in accordance with regulations concerned with recording in working record of violator; 2 - Suspension of working rank and salary promotion as well as suspension of commendation; 3 - Dismissal or demotion of position to work at the lower position; 4 - Dismissal from the status of civil servant without any providing benefits. The staff personnel persons, officials subject to disciplinary must return all the wrongfully acquired assets to the organization they belong to. Article 60. Fining Measures Person, legal entity or organization violating this law shall be subjected of fine in the following cases: 1 - Supplying incorrect data and information to officials and authorities concerned causing damage to any person, legal entity or organization; 2 - None supplying data and information to officials and authorities concerned or defined time or period;

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	3 - Deleting data and information in the computer system or in other computers of person, legal entity or organization without any authorization; 4 - Violating the other prescribed principles in laws and regulations which is an administrative principle violating. The rates of fining for each respective prescribed case are defined in the other specific regulation. Article 61. Civil Measures Person, legal entity and organization violating this law without causing damage to other persons shall be subjected to bear the damage compensation basing on the actual damages they have caused. Article 62. Criminal Measures Any person who commits an offence of cyber crime shall be subjected of punishment as following: 1 - Disclosing of Specific Computer Access Prevention Measure shall be punished by imprisonment from one month to one year with fining from Kip 1.000.000 Kip up to 4.000.000 Kip 2 - Unauthorized Computer Access shall be punished by imprisonment from three months to one year with fining from Kip 2.000.000 Kip up to 20.000.000 Kip; 3 - Unauthorized Editing Picture, Animation, Audio and Video shall be punished by imprisonment from three months to two years with fining from Kip 3.000.000 Kip up to 10.000.000 Kip; 4 - Unauthorized Interception of Computer's Data and Information shall be punished by imprisonment from three months to three years with fining from Kip 4.000.000 kip up to 20.000.000 Kip; 5 - Causing Damages via Online Social Media shall be punished by imprisonment from three months to three years with fining from Kip 4.000.000 Kip up to 20.000.000 Kip; 6 - Dissemination of Pornography shall be punished by imprisonment from one year to five years with fining from Kip 5.000.000 Kip up to 30.000.000 Kip; 7 - Computer System Interference shall be punished by imprisonment from one year to five years with fining from Kip 5.000.000 Kip up to 30.000.000 Kip; 8 - Computer's Data and Information Forgery shall be punished by imprisonment from one year to five years with fining from Kip 5.000.000 Kip up to 30.000.000 Kip;

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	9 - Destroying Computer's Data and Information shall be punished by imprisonment from three years to five years with fining from Kip 10.000.000 Kip up to 50.000.000 Kip; 10 - Operating Business of Tools and Equipments for Cyber Crime shall be punished by imprisonment from three years to five years with fining from Kip 10.000.000 Kip up to 50.000.000 Kip.
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,	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 42. Causes for Opening of Investigation Causes for Opening of cyber crime case are as following: 1 - Having a claim, reporting or complaint of person, legal entity or organization concerning of any offence regarding as cyber crime; 2 - Capitulating of cyber crime perpetrators; 3 - Discovering of cyber crime trace, evidence as well as data and information concerned for the offences prescribed in the Article 8 of this law. Article 43. Process of Investigation of Cyber Crime Case The investigation of cyber crime case shall be conducted as follows: 1 - Claiming, reporting or complaining; 2 - Opening of investigation; 3 - Conducting of investigation; 4 - Summarizing of investigation and preparation of case file

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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 44. Claiming, reporting or complaining The claiming, reporting or complaining an offence regarding as cyber crime shall be brought to notify or submit to the investigation organization of police or office of public prosecutor. The organization of police or office of public prosecutor shall study and consider the claiming, reporting or complaining within five official working days from the day of receiving the claiming, reporting or complaining. In case of having any difficulty, the study and consideration period shall not be more than ten official working days.
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	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 45. Opening of investigation In case of having sufficient information and evidence of any offence regarding as a cyber crime, the head of investigation organization of police or public prosecutor shall issue the ordinance of opening of investigation basing on the scope of rights and duties of the issuing the ordinance in according to the Law on Criminal Procedure. In case of emergency, necessity and having sufficient information and evidence proving that there is a preparation or committing of cyber crime, the head of investigation organization of police or public prosecutor shall issue an ordinance for protection and storage computer's data and information as well computer

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.	traffic data. Service providers or sectors having duties of data and information management have obligations of protection and storage the prescribed data and information in good condition till the final process of cyber crime case procedure in order to ensure that they are not being lost or damaged. Article 46. Conducting of Investigation The investigation organization of police or office of public prosecutor shall coordinate with sector of post and telecommunication and other sectors concerned in order to search and trace information and evidence as well as source of cyber crime for regarding as the basis of investigation conducting. The conducting of cyber crime case investigation shall apply the investigation procedures and the prevention measures as prescribed under the Law on Criminal Procedures.
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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 45. Opening of investigation In case of having sufficient information and evidence of any offence regarding as a cyber crime, the head of investigation organization of police or public prosecutor shall issue the ordinance of opening of investigation basing on the scope of rights and duties of the issuing the ordinance in according to the Law on Criminal Procedure. In case of emergency, necessity and having sufficient information and evidence proving that there is a preparation or committing of cyber crime, the head of investigation organization of police or public prosecutor shall issue an ordinance for protection and storage computer's data and information as well computer traffic data. Service providers or sectors having duties of data and information management have obligations of protection and storage the prescribed data and information in

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	good condition till the final process of cyber crime case procedure in order to ensure that they are not being lost or damaged. Article 46. Conducting of Investigation The investigation organization of police or office of public prosecutor shall coordinate with sector of post and telecommunication and other sectors concerned in order to search and trace information and evidence as well as source of cyber crime for regarding as the basis of investigation conducting. The conducting of cyber crime case investigation shall apply the investigation procedures and the prevention measures as prescribed under the Law on Criminal Procedures.
Article 18 – Production order 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a the type of communication service used, the technical provisions taken thereto and the period of service; b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 45. Opening of investigation In case of having sufficient information and evidence of any offence regarding as a cyber crime, the head of investigation organization of police or public prosecutor shall issue the ordinance of opening of investigation basing on the scope of rights and duties of the issuing the ordinance in according to the Law on Criminal Procedure. In case of emergency, necessity and having sufficient information and evidence proving that there is a preparation or committing of cyber crime, the head of investigation organization of police or public prosecutor shall issue an ordinance for protection and storage computer's data and information as well computer traffic data. Service providers or sectors having duties of data and information management have obligations of protection and storage the prescribed data and information in good condition till the final process of cyber crime case procedure in order to ensure that they are not being lost or damaged. Article 46. Conducting of Investigation

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	The investigation organization of police or office of public prosecutor shall coordinate with sector of post and telecommunication and other sectors concerned in order to search and trace information and evidence as well as source of cyber crime for regarding as the basis of investigation conducting. The conducting of cyber crime case investigation shall apply the investigation procedures and the prevention measures as prescribed under the Law on Criminal Procedures.
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data; d render inaccessible or remove those computer data in the accessed computer system. 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied	.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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:	

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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.	
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	Penal Law of Lao People's Democratic Republic of 2005 Article 3. (New) Application of Penal Law within the Territory of the Lao People's Democratic Republic This law is binding in the territory of the Lao People's Democratic Republic. An individual who commits an offence within the territory of the Lao People's Democratic Republic may be charged and punished in accordance with the Penal Law or other laws of the Lao People's Democratic Republic that define criminal penalties. In the event that diplomatic representatives or individuals benefiting from the diplomatic immunity conferred by international conventions commit offences in the territory of the Lao People's Democratic Republic, these cases shall be solved through diplomatic channels.

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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 4. Application of Penal Law outside the Territory of the Lao People's Democratic Republic Lao citizens who commit offences outside the territory of the Lao People's Democratic Republic shall be charged with and punished for such offences if they are defined [as offences under] the Penal Law of the Lao People's Democratic Republic. Aliens and apatrids residing in the Lao People's Democratic Republic who commit offences outside the territory of the Lao People's Democratic Republic shall also be charged and punished. Foreign individuals who commit offences outside the territory of the Lao People's Democratic Republic shall be charged and punished as provided in the Penal Law of the Lao People's Democratic Republic if such a case is provided for in international conventions.
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	

Back to the Table of Contents

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.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 33. Principle of International Cooperation International cooperation in Campaign of Prevention and Combating Cyber Crime between organizations having authorities concerned of the Lao PDR and foreign organizations should follow the principle of respecting of independence, sovereignty and territorial integrity, non-interference in each other's domestic affair, mutual obtaining benefits and conformity with international agreements and treaties which the Lao PDR is party to.

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 35. Mutual Legal Assistance Mutual Legal Assistance shall be aimed at the requests for conducting of investigation, applying of counting measures, issuing of ordinance for storage and protection of computer's data and information as well as computer traffic data, searching, diagnosing and identifying of offences, request for additional information and evidence related to offences as well as request for extradition. The mechanism and procedure of Mutual Legal Assistance shall follow the related laws and regulation of the Lao PDR, international agreements and treaties, which the Lao PDR is party to. Article 26. Content of the request for Mutual Legal Assistance Request for Mutual Legal Assistance shall include the following contents: 1 - Purpose, necessity reasons and de facto condition of the request; 2 - Any important information necessary for identifying and tracing and diagnosing of cyber crime offenders; 3 - Brief summarizing of computer system's data and information or computer traffic data wanting to protect and storage; 4 - Legislative references and basis towards offences of the accused and the suspect; 5 - Information of organizations or authorities concerned for the case of asking for any additional information from the requesting state.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	
Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution. b The central authorities shall communicate directly with each other; c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph; d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times. 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party. 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary. 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly. 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party. b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol). c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so. d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party. e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 28 – Confidentiality and limitation on use 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof. 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is: a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or b not used for investigations or proceedings other than those stated in the request. 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it. 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.	Law on Prevention and Combating Cyber Crime No. 61/NA of 15 July 2015 Article 37. Requirement of Confidentiality The Competent authority of the Lao PDR must ensure the confidentiality of requests from the related states.
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data. 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation. 4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled. 5 In addition, a request for preservation may only be refused if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests. 6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed. 4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.	
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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted. 2 Disclosure of traffic data under paragraph 1 may only be withheld if: a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.	
Article 31 – Mutual assistance regarding accessing of stored computer data 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29. 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter. 3 The request shall be responded to on an expedited basis where: a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.	
Article 32 – Trans-border access to stored computer data with consent or where publicly available A Party may, without the authorisation of another Party: a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and 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	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law. 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.	
Article 34 – Mutual assistance regarding the interception of content data The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.	
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. 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.	

Back to the Table of Contents

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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