

Thailand

Cybercrime legislation

Domestic equivalent to the provisions of the Budapest Convention

Table of contents

Version 3 June 2020

[reference to the provisions of the Budapest Convention]

Chapter I - Use of terms

Article 1 - "Computer system", "computer data", "service provider", "traffic data"

Chapter II - Measures to be taken at the national level

Section 1 – Substantive criminal law

Article 2 - Illegal access

Article 3 - Illegal interception

Article 4 - Data interference

Article 5 - System interference

Article 6 - Misuse of devices

Article 7 - Computer-related forgery

Article 8 - Computer-related fraud

Article 9 - Offences related to child pornography

Article 10 – Offences related to infringements of copyright and related rights

Article 11 – Attempt and aiding or abetting

Article 12 - Corporate liability

Article 13 - Sanctions and measures

Section 2 - Procedural law

Article 14 - Scope of procedural provisions

Article 15 – Conditions and safeguards

Article 16 - Expedited preservation of stored computer data

Article 17 - Expedited preservation and partial disclosure of traffic data

Article 18 - Production order

Article 19 – Search and seizure of stored computer data

Article 20 - Real-time collection of traffic data

Article 21 - Interception of content data

Section 3 – Jurisdiction

Article 22 - Jurisdiction

Chapter III – International co-operation

Article 24 - Extradition

Article 25 – General principles relating to mutual assistance

Article 26 – Spontaneous information

Article 27 - Procedures pertaining to mutual assistance requests in the

absence of applicable international agreements

Article 28 - Confidentiality and limitation on use

Article 29 - Expedited preservation of stored computer data

Article 30 - Expedited disclosure of preserved traffic data

Article 31 – Mutual assistance regarding accessing of stored computer

aata

Article 32 – Trans-border access to stored computer data with consent or

where publicly available

Article 33 - Mutual assistance in the real-time collection of traffic data

Article 34 - Mutual assistance regarding the interception of content data

Article 35 – 24/7 Network

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.



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

DOMESTIC LEGISLATION

Chapter I – Use of terms

Article 1 – "Computer system", "computer data", "service provider", "traffic data":

For the purposes of this Convention:

- a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
- c "service provider" means:
- i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
- ii any other entity that processes or stores computer data on behalf of such communication service or users of such service:
- d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service

Computer Crime Act (2007, amended 2017) (henceforth CCA)

Section 3

In this Act,

"Computer System" means a piece of equipment or sets of equipment units, whose function is integrated together, for which set of instructions and working principles enable it or them to perform the duty of processing data automatically.

"Computer Data" means data, statements, or set of instructions contained in a computer system, the output of which may be processed by a computer system including electronic data, according to the Law of Electronic Transactions.

"Computer Traffic Data" means data related to computer system-based communications showing sources of origin, starting points, destinations, routes, time, dates, volumes, time periods, types of services or others related to that computer system's communications.

"Service Provider" means:

- (1) A person who provides service to the public with respect to access to the Internet or other mutual communication via a computer system, whether on their own behalf, or in the name of, or for the benefit of, another person (2) A person who provides services with respect to the storage of computer data for the benefit of the other person
- "Service User" means a person who uses the services provided by a service provider, with or without fee.

DOMESTIC LEGISLATION

"Competent Official" means a person appointed by a Minister to perform duties under this Act.

"Minister" means a Minister who has responsibility and control for the execution of this Act.

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 Section 5 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.

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.

CCA (2007, amended 2017) Chapter I: Computer related offenses

Any person who illegally accesses a computer system for which a specific access prevention measure that is not intended for their own use is available shall be subject to imprisonment not exceeding six months or a fine not exceeding ten thousand baht, or both.

Section 7

Any person who illegally accesses computer data, for which there is a specific access prevention measure not intended for their own use available, then he or she shall be subject to imprisonment not exceeding two years or a fine not exceeding forty thousand baht, or both.

CCA (2007, amended 2017) Chapter I: Computer related offenses

Section 8

Any person who illegitimately perpetrates any act by electronic means to intercept computer data of other people during its transmission in a computer system, and that computer data is not intended for the public interest or the use of general people, shall be subject to imprisonment not exceeding three years or a fine not exceeding sixty thousand baht, or both.

Telecommunications Business Act B.E. 2544 (2001), Chapter X: Penalty provisions

Section 74

Any person who commits an act by any means to illegally intercept, utilize or disclose news or message or any other information communicated via telecommunications shall be liable to imprisonment for a term of not exceeding

BUDAPEST CONVENTION DOMESTIC LEGISLATION two years or toa fine not exceeding four hundred thousand baht or to both. CCA (2007, amended 2017) Chapter I: Computer related offenses Article 4 - Data interference 1 Each Party shall adopt such legislative and other measures as may be Section 9 necessary to establish as criminal offences under its domestic law, when Any person who illegitimately damages, destroys, alters, changes, or amends committed intentionally, the damaging, deletion, deterioration, alteration or computer data of other people, either in whole or in part, shall be subject to suppression of computer data without right. imprisonment not exceeding five years or a fine not exceeding one hundred 2 A Party may reserve the right to require that the conduct described in thousand baht, or both. paragraph 1 result in serious harm. **Article 5 - System interference** CCA (2007, amended 2017) Chapter I: Computer related offenses Each Party shall adopt such legislative and other measures as may be Section 10 necessary to establish as criminal offences under its domestic law, when Any person who illegitimately perpetrates any act that causes the working of committed intentionally, the serious hindering without right of the computer system of other people to be suspended, delayed, hindered or functioning of a computer system by inputting, transmitting, damaging, disrupted to the extent that the computer system fails to operate normally shall deleting, deteriorating, altering or suppressing computer data be subject to imprisonment not exceeding five years or a fine not exceeding one hundred thousand baht, or both. Section 11 Any person who sends computer data or electronic mail to another person and covering up the source of such aforementioned data in a manner that disturbs the other person's normal operation of their computer system shall be subject to a fine not exceeding one hundred thousand baht. Any person who sends computer data or electronic mail to another person causing a nuisance to the recipient of such computer data or electronic mail, without a convenient option for the recipient to terminate the reception or to express their intent to refuse the reception, shall be subject to a fine not exceeding two hundred thousand baht. The Minister shall issue a Ministerial Notification prescribing the nature and

method of sending, as well as the nature and volume of computer data or electronic mail, which are deemed not to cause nuisance to the recipient; and prescribing the nature of a convenient option to terminate the reception or to

express an intent to refuse the reception.

Section 12

BUDAPEST CONVENTION DOMESTIC LEGISLATION If the perpetration of an offense under Section 5, or 6, or 7, or 8 or 11 is an act upon computer data or a computer system related to the maintenance of national security, public safety, national economic security, or infrastructure serving public interest, the perpetrator shall be subject to imprisonment from one year up to seven years and a fine of twenty thousand baht up to one hundred and forty thousand baht. If the perpetration of such offense under Paragraph One has caused damage to the computer data or the computer system, the perpetrator shall be subject to imprisonment from one year up to ten years and a fine of twenty thousand baht up to two hundred thousand baht. If the perpetration of an offense under Section 9 or 10 is an act upon computer data or a computer system according to Paragraph One, the perpetrator shall be subject to imprisonment from three years up to fifteen years and a fine of sixty thousand baht up to three hundred thousand baht. If the perpetration of an offense under Paragraph One or Paragraph Three, albeit without intent to kill, has resulted in the death of other person, the perpetrator shall be subject to imprisonment from five years up to twenty years and a fine of one hundred thousand baht up to four hundred thousand baht. **Section 12/1.** If the commission of an offence under section 9 or section 10 causes injury to another person or any property of another person, the offender shall be liable to imprisonment for a term not exceeding ten years and to a fine not exceeding two hundred thousand Baht. If the commission of an offence under section 9 or section 10 is without any intent to murder but causes death of another person, the offender shall be liable to imprisonment for a term of five years to twenty years and to a fine of one hundred thousand Baht to four hundred thousand Baht." Article 6 - Misuse of devices **CCA** (2007, amended 2017) **Chapter I: Computer related offenses** 1 Each Party shall adopt such legislative and other measures as may be Section 13 necessary to establish as criminal offences under its domestic law, when Any person who sells or disseminates set of instructions developed as a tool committed intentionally and without right: used in perpetrate an offense under Section 5, Section 6, Section 7, Section 8,

DOMESTIC LEGISLATION

a the production, sale, procurement for use, import, distribution or otherwise making available of:

- i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
- ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
- b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
- 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
- 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

Section 9, Section 10 and Section 11 shall be subject to imprisonment for not exceeding one year or a fine not exceeding twenty thousand baht, or both.

Any person who sells or distributes a set of instructions specifically designed as a tool for the perpetration of an offense under Section 12 Paragraph One or Paragraph Three shall be subject to imprisonment not exceeding two years or a fine not exceeding forty thousand baht, or both.

Any person who sells or distributes a set of instructions specifically designed as a tool for the perpetration of an offense under Section 5, or 6, or 7, or 8, or 9, or 10 or 11, if the person who has put it to use is found to have violated Section 12 Paragraph One or Paragraph Three, or culpable as to Section 12 Paragraph Two or Paragraph Four or Section 12/1, the person who sells or distributes such a set of instructions shall receive the higher penalty rate only if they had been aware or could have foreseen such a result.

Any person who sells or distributes a set of instructions specifically designed as a tool for the perpetration of an offense under Sections 12 Paragraph One or Paragraph Three, if the person who has put it to use is found to have violated Section 12 Paragraph One or Paragraph Three, or culpable as to Section 12 Paragraph Two or Paragraph Four or Section 12/1, the person who sells or distributes such a set of instructions shall receive the higher penalty rate.

If a person who sells or distributes the set of instructions is found guilty as per Paragraph One or Two and Paragraph Three or Four as well, the person shall be sentenced to the highest penalty rate for one count.

CCA (2007, amended 2017) **Chapter II: Competent officials**

Section 21

If a competent official found that any computer data contains undesirable set of instructions, the competent official may file a petition, to the court of jurisdiction, for a court order to prohibit the sale or the dissemination of that computer data; or to instruct the person who owns or possesses that computer data to suspend the use, destroy, or correct the computer data; or to impose a condition with respect to the use, possession, or dissemination of the

DOMESTIC LEGISLATION

undesirable set of instructions.

The undesirable set of instructions under Paragraph One shall refer to a set of instructions which causes a computer data, a computer system, or other sets of instructions to be damaged, destroyed, altered or appended, malfunction or failed to perform according to instructions, or otherwise as prescribed in Ministerial Regulations. The exception shall be made to an undesirable set of instructions that may be used for the prevention or the correction of the foregoing set of instructions. The Minister may publish in the Government Gazette, prescribing list of names, characteristics, or details of the undesirable set of instructions which can be used to prevent or correct the undesirable set of instructions.

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, 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.

<u>CCA</u> (2007, amended 2017) **Chapter I: Computer related offenses Section 14**

Any person who perpetrates the following offenses shall be subject to imprisonment up to five years and a fine not exceeding one hundred thousand baht, or both:

- (1) with ill or fraudulent intent, put into a computer system distorted or forged computer data, partially or entirely, or false computer data, in a manner that is likely to cause damage to the public, in which the perpetration is not a defamation offense under the Criminal Code;
- (2) put into a computer system false computer data in a manner that is likely to damage the maintenance of national security, public safety, national economic security or public infrastructure serving national's public interest or cause panic in the public;
- (3) put into a computer system any computer data which is an offense about the security of the Kingdom or is an offense about terrorism, according to Criminal Code;
- (4) put into a computer system any computer data which is obscene and that computer data may accessible by the public;
- (5) disseminate or forward any computer data when being aware that it was the computer data as described in (1), (2), (3) or (4).

If the offense under Paragraph One (1) has not been perpetrated against the

DOMESTIC LEGISLATION

public but against a particular individual, the perpetrator or a person who distributes or transfer the computer data shall be subject to imprisonment not exceeding three years and a fine not exceeding sixty thousand baht, or both, and it is a compoundable offense.

Section 15

Any service provider who cooperates, consents or acquiesces to the perpetration of an offense under Section 14 within a computer system under their charge shall be subject to the same penalty as that imposed upon a person perpetrated an offense under Section 14.

The Minister shall issue a Ministerial Notification prescribing procedural steps of for the notification, the suppression of the dissemination of such data, and the removal of such data from a computer system.

If the service provider can prove a compliance to such Ministerial Notification issued by the Minister as per Paragraph Two had been made, they shall be exempted from penalty.

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.

Thailand Criminal Code B.E. 2499 (1956) amended Criminal Code No. 17 B.E. 2547 (2003), Title XII: Offences against property, Chapter 3: Offences of cheating and fraud Section 341

Whoever, dishonestly deceives a person with the assertion of a falsehood or the concealment of the facts which should be revealed, and, by such deception, obtains a property from the person so deceived or a third person, or causes the person so deceived or a third person to execute, revoke or destroy a document of right, is said to commit the offence of cheating and fraud, and shall be punished with imprisonment not exceeding three years or fined not exceeding six thousand Baht, or both.

Section 342

If the offence of cheating and fraud be committed:

- (1) By the offender showing himself to be another person; or
- (2) By taking advantage of the lack of intelligence of the deceived person who is a child, or by taking advantage of weakness of mind of the deceived person,

DOMESTIC LEGISLATION

The offender shall be punished with imprisonment not exceeding five years or fined not exceeding ten thousand Baht, or both.

Section 344

Whoever, dishonestly, deceiving ten persons upwards to perform any work for oneself or for the third person with the intent not to pay the wages or remuneration to such persons, or with the intent to pay such persons lower wages or remuneration than those agreed upon, shall be imprisoned not out of three years or fined not out of six thousand Baht, or both.

Section 346

Whoever, in order to take a property of another person for himself or a third person, induces any person to dispose of the property at a disadvantage on account of the induced person being weak-minded, or being a child lacking in intelligence and being unable to understand reasonably the essentials of his acts so that the induced person submits to the disposal of such property, shall be punished with imprisonment not exceeding two years or fined not exceeding four thousand Baht, or both.

Section 347

Whoever, so as to oneself or the other person to obtain the benefit the insurance, maliciously causing the danger to the insured property, shall be imprisoned not out of five years or fined not out of to thousand Baht, or both.

Title I: Provisions applicable to general offences, Chapter 4: Criminal liability

Section 71

If the offences as provided in Section 334 to Section 336, first paragraph, and Section 341 to Section 364 are committed by a husband against his wife, or by a wife against her husband, the offender shall not be punished.

If the aforesaid offences are committed by an ascendant against his descendant, or by a descendant against his ascendant, or by a brother or sister of the same parents against each other, the offences shall, even though not provided by the law as compoundable offences, be deemed as compoundable offences.

DOMESTIC LEGISLATION

Moreover, the Court may inflict less punishment to any extent than that provided by the law for such offences.

Title 3 - Content-related offences

Article 9 - Offences related to child pornography

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - a producing child pornography for the purpose of its distribution through a computer system;
 - b offering or making available child pornography through a computer system:
 - c distributing or transmitting child pornography through a computer system;
 - d procuring child pornography through a computer system for oneself or for another person;
 - e possessing child pornography in a computer system or on a computer-data storage medium.
- 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:
 - 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 agelimit, 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.

CCA (2007, amended 2017) **Chapter I: Computer related offenses Section 14**

- Any person who perpetrates the following offenses shall be subject to imprisonment up to five years and a fine not exceeding one hundred thousand baht, or both:
- (1) with ill or fraudulent intent, put into a computer system distorted or forged computer data, partially or entirely, or false computer data, in a manner that is likely to cause damage to the public, in which the perpetration is not a defamation offense under the Criminal Code;
- (2) put into a computer system false computer data in a manner that is likely to damage the maintenance of national security, public safety, national economic security or public infrastructure serving national's public interest or cause panic in the public;
- (3) put into a computer system any computer data which is an offense about the security of the Kingdom or is an offense about terrorism, according to Criminal Code;
- (4) put into a computer system any computer data which is obscene and that computer data may accessible by the public;
- (5) disseminate or forward any computer data when being aware that it was the computer data as described in (1), (2), (3) or (4).

If the offense under Paragraph One (1) has not been perpetrated against the public but against a particular individual, the perpetrator or a person who distributes or transfer the computer data shall be subject to imprisonment not exceeding three years and a fine not exceeding sixty thousand baht, or both, and it is a compoundable offense.

Section 15

Any service provider who cooperates, consents or acquiesces to the perpetration of an offense under Section 14 within a computer system under their charge shall be subject to the same penalty as that imposed upon a person perpetrated an offense under Section 14.

BUDAPEST CONVENTION DOMESTIC LEGISLATION The Minister shall issue a Ministerial Notification prescribing procedural steps of for the notification, the suppression of the dissemination of such data, and the removal of such data from a computer system. If the service provider can prove a compliance to such Ministerial Notification issued by the Minister as per Paragraph Two had been made, they shall be exempted from penalty. Child Protection Act B.E. 2546 (2003) Chapter 2: Treatment of the child Section 26 Under the provision of other laws, regardless of a child's* consent, a person is forbidden to acts as follows: 1) Commit or omit acts which result in torturing a child's body or mind; [...] 3) Force, threaten, induce, encourage or allow a child to adopt behavior and manners which are inappropriate or likely to be the cause of wrongdoing; 4) Advertise by means of the media or use any other means of information dissemination to receive or give away a child to any person who is not related to the child, save where such action is sanctioned by the State; 5) Force, threaten, induce, encourage, consent to, or act in a any other way that results in a child becoming a beggar, living on the street, or use a child as an instrument for begging or committing crimes, or act in any way that results in the exploitation of a child; 6) Use, employ or ask a child to work or act in such a way that might be physically or mentally harmful to the child, affect the child's growth or hinder the child's development; 7) Force, threaten, use, induce, instigate, encourage, or allow a child to play sports or commit any acts indicative of commercial exploitation in a manner which hinders the child's growth and development or constitutes an act of torture against the child; [...] 9) Force, threaten, use, induce, instigate, encourage or allow a child to perform or act in a pornographic manner, regardless of whether the intention is to obtain regardless of whether the intention is to obtain remuneration or anything else; [...]

Section 27

BUDAPEST CONVENTION DOMESTIC LEGISLATION It is forbidden for anyone to advertise or disseminate by means of the media or any other kind of information technology any information on a child or the child's guardian, with the intention of causing damage to the mind, reputation, prestige or any other interests of the child or seeking benefit for oneself or others in an unlawful manner. *Section 4 "Child" means a person below 18 years of age, but does not include those who have attained majority through marriage. Title 4 - Offences related to infringements of copyright and related rights Article 10 - Offences related to infringements of copyright and **Copyright Act B.E. 2537** (1994) related rights Ministerial Regulation B.E. 2540 issued under the Copyright Act B.E. Each Party shall adopt such legislative and other measures as may be 2537 necessary to establish as criminal offences under its domestic law the Rules for Intellectual Property and International Trade Cases B.E. 2540 infringement of copyright, as defined under the law of that Party, pursuant (1997)to the obligations it has undertaken under the Paris Act of 24 July 1971 Act on the Establishment of and Procedure for Intellectual Property and revising the Bern Convention for the Protection of Literary and Artistic **International Trade Court B.E. 2539** (1996) 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. 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. 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.

DOMESTIC LEGISLATION

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 Section 15 necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the Convention with intent that such offence be committed.
- 2 Each Party shall adopt such legislative and other measures as may be 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.

CCA (2007, amended 2017) Chapter I: Computer related offenses

Any service provider who cooperates, consents or acquiesces to the perpetration of an offense under Section 14 within a computer system under their charge offences established in accordance with Articles 2 through 10 of the present shall be subject to the same penalty as that imposed upon a person perpetrated an offense under Section 14.

necessary to establish as criminal offences under its domestic law, when The Minister shall issue a Ministerial Notification prescribing procedural steps of for the notification, the suppression of the dissemination of such data, and the removal of such data from a computer system.

> If the service provider can prove a compliance to such Ministerial Notification issued by the Minister as per Paragraph Two had been made, they shall be exempted from penalty.

Thailand Criminal Code B.E. 2499 (1956), Book I, Title I: Provisions applicable to general offences, Chapter 2: Application of criminal laws Section 5

Whenever any offence is even partially committed within the Kingdom, or the consequence of the commission of which, as intended by the offender, occurs within the Kingdom, or by the nature of the commission of which, the consequence resulting therefrom should occur within the Kingdom, or it could be foreseen that the consequence would occur within the Kingdom, it shall be deemed that such offence is committed within the Kingdom.

In case of preparation or attempt to commit any act provided by the law to be an offence, even though it is done outside the Kingdom, if the consequence of the doing of such act, when carried through to the stage of accomplishment of the offence, will occur within the Kingdom, it shall be deemed that the preparation or attempt to commit such offence is done within the Kingdom.

Chapter 5: Of commitment Section 80

Whoever commences to commit an offence, but does not carry it through, or

BUDAPEST CONVENTION DOMESTIC LEGISLATION carries it through, but does not achieve its end, is said to attempt to commit an offence. Whoever attempts to commit an offence shall be liable to two-thirds of the punishment as provided by the law for such offence. Section 81 Whoever commences and commits the offence, but does not commit it through, or commits it through, but does not achieve its good result, such person in said to attempts and commits an offence. The offence is attempted to commit by whomever, such person shall be punished two-thirds of punishment as prescribed by the law for such offence. If the act mentioned in the first paragraph is done on account of blind belief, the Court may not inflict the punishment. Section 82 Whoever attempts to commit an offence, but, on his own accord, desists from carrying it through, or changes his mind and prevents the act from achieving its end, shall not be punished for such attempt to commit the offence. But, if what he has already done comes under the provisions of law as an offence, he shall be punished for such offence. Chapter 6: Principals and supporters Section 86 Whoever does for any reason whatsoever as assist or facilitate to any other person committing an offence before or late time of committing the offence, even though such assistance or support is not known by the offender, such assistance is deemed to be support for committing such offence shall be punished by two-thirds of the punishment as provided for such offence. Article 12 - Corporate liability CCA (2007, amended 2017) Chapter I: Computer related offenses 1 Each Party shall adopt such legislative and other measures as may be Section 15 necessary to ensure that legal persons can be held liable for a criminal Any service provider who cooperates, consents or acquiesces to the perpetration offence established in accordance with this Convention, committed for their of an offense under Section 14 within a computer system under their charge benefit by any natural person, acting either individually or as part of an shall be subject to the same penalty as that imposed upon a person perpetrated organ of the legal person, who has a leading position within it, based on: an offense under Section 14.

a power of representation of the legal person;

DOMESTIC LEGISLATION

- 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.

The Minister shall issue a Ministerial Notification prescribing procedural steps of for the notification, the suppression of the dissemination of such data, and the removal of such data from a computer system.

If the service provider can prove a compliance to such Ministerial Notification issued by the Minister as per Paragraph Two had been made, they shall be exempted from penalty.

<u>Special Case Investigation Act B.E. 2547</u> (2004), Chapter III: Special case investigation and inquiry Section 21

Special Cases required to be investigated and examined according to this Act are the following criminal cases:

- (1) Criminal cases according to the laws provided in the Annex attached hereto and in the ministerial regulations as recommended by the Board Special Case (BSC) where such criminal cases shall have any of the following natures:
- (a) It is a complex criminal case that requires special inquiry, investigation and special collection of evidence.
- (b) It is a criminal case which has or might have a serious effect upon public order and moral, national security, international relations or the country's economy or finance.
- (c) It is a criminal case which is a serious transnational crime or committed by an organized criminal group.
- (d) It is a criminal case in which influential person being a principal, instigator or supporter.
- (e) It is a criminal case in which the Administrative Official or Senior Police Officer, who is neither the Special Case Inquiry Official nor Special Case Officer, is the suspect as there is reasonable evidence of crime committed, or being the alleged culprit, or being the accused.

This however shall be in line with details of the offence provided by the BSC.

(2) Criminal cases other than those stated in (1) where the BSC resolves by no less than two-thirds votes of its existing Board members.

In a case of a single offence against various legal provisions and a particular provision is handled by a Special Case Inquiry Official according to this Act, or in a case of several related or continuous offences and a particular offence is

BUDAPEST CONVENTION DOMESTIC LEGISLATION handled by the Special Case Inquiry Official according hereto, such Special Case Inquiry Official shall have the power to investigate offences against such other provisions or other matters and such cases shall be considered as a Special Case. Any case in which the investigation has already been completed by a Special Case Inquiry Official shall be considered as a Special Case Investigation according hereto. This provision shall also apply to a person who becomes a principal, instigator or supporter of an offence. In the case where there is dispute or doubt over whether a crime is a special case provided in paragraph one (1) or not, the BSC shall be the arbiter. Laws Provided in the Annex Attached to the Special Case Investigation Act B.E. 2547 (2004) 1. Law on Loan Amounting to Public Cheating and Fraud 2. Competition Act 3. Commercial Banking Act 4. Law on the Finance Business Securities Business and Credit Foncier Business 5. Chain Loan Control Act 6. Foreign Exchange Control Act 7. Law on Government Procurement Fraud 8. Act for the Protection of Layout-Designs of Integrated Circuits 9. Consumer Protection Act 10. Trademark Act 11. Currency Act 12. Tax and Duty Compensation of Exported Goods Produced in the Kingdom Act 13. Interest on Loan by the Financial Institution Act 14. Bank of Thailand Act 15. Public Company Act 16. Anti Money Laundering Act 17. The Industrial Product Standard Act 18. Copyright Act 19. Board of Investment Commission Act 20. Enhancement and Conservation of National Environmental Quality Act

BUDAPEST CONVENTION DOMESTIC LEGISLATION 21. Patent Act 22. Security and Exchange Commission Act 23. Revenue Code 24. Customs Law 25. Excise Law 26. Liquor Act 27. Tabacco Act 28. Foreign Business Act 29. Casualty Insurance Act 30. Life Insurance Act 31. Law on Agricultural Futures Trading 32. Computer Crime Act 33. Land Law 34. Forest Law 35. National Park Act 36. National Reserved Forest Act 37. Wildlife Preservation and Protection Act Article 13 - Sanctions and measures > BC Article 2 = CCA: Chapter I, Section 5; Section 7 Each Party shall adopt such legislative and other measures as may be > BC Article 3 = CCA: Chapter I, Section 8; Telecommunications necessary to ensure that the criminal offences established in accordance Business Act B.E. 2544 (2001), Chapter X, Section 74 with Articles 2 through 11 are punishable by effective, proportionate and > BC Article 4 = CCA: Chapter I, Section 9; dissuasive sanctions, which include deprivation of liberty. > BC Article 5 = CCA: Chapter I, Sections 10-12/1; Each Party shall ensure that legal persons held liable in accordance > BC Article 6 = CCA: Chapter I, Section 13; with Article 12 shall be subject to effective, proportionate and dissuasive > BC Article 7 = CCA: Chapter I, Section 14 - 15; criminal or non-criminal sanctions or measures, including monetary > BC Article 8 = Thailand Criminal Code B.E. 2499 (1956) amended Criminal Code No. 17 B.E. 2547 (2003), Title XII, Chapter 3, Sections sanctions. 341, 342, 344, 346, 347, 348; > BC Article 9 = CCA: Chapter I, Section 14 - 15; Child Protection Act **B.E. 2546** (2003) Chapter 9: Penalties, Section 78 - 79; > **BC Article 10 = Copyright Act B.E. 2537** (1994), Chapter 8: Penalties; > BC Article 11 = CCA: Chapter I, Section 15; Thailand Criminal Code

B.E. 2499 (1956), Book I, Title I, Section 86

BUDAPEST CONVENTION DOMESTIC LEGISLATION Section 2 - Procedural law Article 14 - Scope of procedural provisions **CCA** (2007, amended 2017) 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: the criminal offences established in accordance with Articles 2 а through 11 of this Convention: other criminal offences committed by means of a computer system: and 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: is being operated for the benefit of a closed group of users, and does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to

enable the broadest application of the measures referred to in Articles 20

Article 15 – Conditions and safeguards

and 21

CCA (2007, amended 2017) Chapter II: Competent officials

- 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.

DOMESTIC LEGISLATION

Section 19

In the exercise of power of the competent official under Section 18 (4), (5), (6), (7), and (8), the competent official shall file a petition to the court of jurisdiction for a court order to authorize the competent official to take action. The petition must identify a reasonable ground to believe that the person is perpetrating or going to perpetrate an offense under this Act, reasons for the exercise of such power, characteristics of the offense, description of the devices used for perpetrating the offense and of the alleged offender, as much as this can be identified. The court should adjudicate urgently such aforementioned petition.

When the court approves permission, and before taking any action according to the court order, the competent official shall submit a copy of the reasonable ground memorandum to show that an authorization under Section 18 (4), (5), (6), (7) and (8), must be employed against the owner or possessor of the computer system, as evidence thereof. If there is no owner of such computer thereby, the competent official should submit a copy of said memorandum as soon as possible.

In order to take action under Section 18 (4), (5), (6), (7) and (8), the senior officer of the competent official shall deliver a copy of the memorandum about the description and rationale of the operation to the court of jurisdiction within forty eight (48) hours after the action has been taken as evidence thereof.

When copying computer data under Section 18 (4), and given that it may be done only when there is a reasonable ground to believe that there is an offense against this Act, such action must not excessively interfere or obstruct the business operation of the computer data's owner or possessor.

Regarding seizure or attachment under Section 18 (8), a competent official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. This is provided, however, that the seizure or attachment shall not last longer than thirty days. If seizure or attachment requires a longer time period, a petition shall be filed at the court of jurisdiction for the extension of the seizure or attachment time period. The court may allow only one or several time extensions, however altogether for no longer than sixty days. When that seizure or attachment is no longer necessary, or upon its expiry date, the competent official must immediately return the computer

BUDAPEST CONVENTION DOMESTIC LEGISLATION system that was seized or withdraw the attachment. The letter of seizure or attachment under Paragraph Five shall be in accordance with a Ministerial Regulation. Section 20 When there is an action to disseminate computer data as follows, the competent official, with approval from the Minister, may file a petition with supporting evidence, to the court of jurisdiction, for a court order to suppress the dissemination or to remove such computer data from a computer system. (1) Computer data actionable per this Act; (2) Computer data which may compromise the security of the Kingdom as prescribed in Book II Title 1 or Title 1/1 of the Criminal Code: (3) Computer data which is a criminal offense per laws related to intellectual property or other laws, where such computer data is a breach to the public order or moral high ground of the people, and the law enforcement official or the inquiry official per the Criminal Procedure Code has made a request about. When there is an action to disseminate computer data which is appropriate to be a breach to the public order or moral high ground of the people, the Minister, with approval of the Computer Data Screening Committee, may authorize a competent official to file a petition with supporting evidence to the court of iurisdiction for a court order to suppress the dissemination or to remove such computer data from a computer system. The meeting of the Computer Data

The Minister shall appoint one or more of Computer Data Screening Committee per Paragraph Two. Each committee shall be consisted of nine members, three of whom must come from private sector in the fields of human rights, mass communication, information technology, or other relevant fields. The committee members shall be remunerated as per the criteria prescribed by the Minister with approval from the Ministry of Finance.

Screening Committee shall be governed by provisions on the committee authorized to carry out administrative procedure under the administrative

procedure law mutatis mutandis.

The act of the court per Paragraph One and Paragraph Two shall be guided by the Criminal Procedure Code mutatis mutandis. When the court issues an order

DOMESTIC LEGISLATION

to suppress the dissemination or to remove such computer data per Paragraph One or Paragraph Two, the competent official may suppress the dissemination or remove the computer data themselves or instruct the service provider to suppress the dissemination or remove the computer data. The Minister shall issue a Ministerial Notification prescribing the criteria, duration, and procedure to suppress the dissemination or to remove the computer data, for the competent official and the service provider, and they shall be made compatible to each other, with the consideration of the changing technological development, unless the court had instructed otherwise.

In case of necessity and emergency, the competent official may file the petition for the court order per Paragraph One before obtaining any approval from the Minister, and the competent official with approval from the Computer Data Screening Committee may file the petition for the court order per Paragraph Two before obtaining any authorization from the Minister, but it is obliged that they urgently bring the matter to the attention of the Minister.

Section 21

If a competent official found that any computer data contains undesirable set of instructions, the competent official may file a petition, to the court of jurisdiction, for a court order to prohibit the sale or the dissemination of that computer data; or to instruct the person who owns or possesses that computer data to suspend the use, destroy, or correct the computer data; or to impose a condition with respect to the use, possession, or dissemination of the undesirable set of instructions.

The undesirable set of instructions under Paragraph One shall refer to a set of instructions which causes a computer data, a computer system, or other sets of instructions to be damaged, destroyed, altered or appended, malfunction or failed to perform according to instructions, or otherwise as prescribed in Ministerial Regulations. The exception shall be made to an undesirable set of instructions that may be used for the prevention or the correction of the foregoing set of instructions. The Minister may publish in the Government Gazette, prescribing list of names, characteristics, or details of the undesirable set of instructions which can be used to prevent or correct the undesirable set of instructions.

BUDAPEST CONVENTION DOMESTIC LEGISLATION Constitution of the Kingdom of Thailand 2017 Section 31 (freedom of religion) A person shall enjoy full liberty to profess a religion, and shall enjoy the liberty to exercise or practice a form of worship in accordance with his or her religious principles, provided that it shall not be adverse to the duties of all Thai people, neither shall it endanger the safety of the State, nor shall it be contrary to public order or good morals. Section 32 (privacy) A person shall enjoy the rights of privacy, dignity, reputation and family. Any act violating or affecting the right of a person under paragraph one, or exploitation of personal information in any manner whatsoever shall not be permitted, except by virtue of a provision of law enacted only to the extent of necessity of public interest. **Section 34** (freedom of expression) A person shall enjoy the liberty to express opinions, make speeches, write, print, publicise and express by other means. The restriction of such liberty shall not be imposed, except by virtue of the provisions of law specifically enacted for the purpose of maintaining the security of the State, protecting the rights or liberties of other persons, maintaining public order or good morals, or protecting the health of the people. [...] **Section 35** (freedom of the press) A media professional shall have liberty in presenting news or expressing opinions in accordance with professional ethics. The closure of a newspaper or other mass media in deprivation of the liberty under paragraph one shall not be permitted. Censorship by a competent official of any news or statements made by a media professional before the publication in a newspaper or any media shall not be permitted, except during the time when the country is in a state of war. The owner of a newspaper or other mass media shall be a Thai national. No grant of money or other properties shall be made by the State as subsidies to private newspapers or other private mass media. A State agency which pays money or gives properties to mass media, regardless of whether it is for the

purpose of advertisement or public relations, or for any other similar purpose, shall disclose the details to the State Audit Commission within the prescribed

BUDAPEST CONVENTION DOMESTIC LEGISLATION period of time and shall also announce them to the public. A State official who performs mass media duties shall enjoy the liberties under paragraph one, provided that the purposes and missions of the agency to which he or she is attached shall also be taken into consideration. **Section 36** (freedom of speech) A person shall enjoy the liberty of communication by any means. Censorship, detention or disclosure of information communicated between persons, including any commission of an act carried out to know or obtain information communicated between persons, shall not be permitted, except by an order or a warrant issued by the Court or where there are other grounds as prescribed by law. **Section 38** (freedom of movement) A person shall enjoy the liberty of travelling and the liberty of making the choice of his or her residence. The restriction of such liberties under paragraph one shall not be imposed except by virtue of a provision of law enacted for the purpose of security of the State, public order, public welfare or town and country planning, or for maintaining family status, or for welfare of youth. **Section 42** (freedom of association) A person shall enjoy the liberty to unite and form an association, co-operative, union, organisation, community, or any other group. The restriction of such liberty under paragraph one shall not be imposed except by virtue of a provision of law enacted for the purpose of protecting public interest, for maintaining public order or good morals, or for preventing or eliminating barriers or monopoly. **Section 44** (freedom of assembly) A person shall enjoy the liberty to assemble peacefully and without arms. The restriction of such liberty under paragraph one shall not be imposed except

or liberties of other persons.

Special Case Investigation Act B.E. 2547 (2004), Chapter III: Special

by virtue of a provision of law enacted for the purpose of maintaining security of the State, public safety, public order or good morals, or for protecting the rights

BUDAPEST CONVENTION DOMESTIC LEGISLATION case investigation and inquiry Section 25 In cases where there is a reasonable ground to believe that any document or information sent by post, telegram, telephone, facsimile, computer, communication device or equipment or any information technology media has been or may be used to commit a Special case offence, the Special Case Inquiry Official approved by the Director-General in writing may submit an ex parte application to the Chief Judge of the Criminal court asking for his/her order to permit the Special Case Inquiry Official to obtain such information. When granting permission under paragraph one, the Chief Judge of the Criminal Court shall consider the effect on individual rights or any other right in conjunction with the following reasons and necessities: (1) there is a reasonable ground to believe that an offence of a Special Case is or will be committed: (2) there is a reasonable ground to believe that access to the information will result in getting the information of a Special Case offence; and (3) there is no more appropriate or efficient method. The Chief Judge of the Criminal Court may grant permission under paragraph one for a period of no more than 90 days each time with any condition. For the purpose of this Section, any person related to the information stated in the media under such an order is required to cooperate. After the permission, if it

he/she shall report that action to the Chief Judge of the Criminal Court for acknowledgement.

After the Special Case Inquiry Official has executed according to the permission,

appears that the fact or a necessity is not as provided, or if there is any change in circumstances, the Chief Judge of the Criminal Court may change such

permission order as appropriate.

Only information acquired under paragraph one which is related to a Special Case offence as permitted under paragraph one shall be kept and used as evidence in the proceedings of such special cases only. Other information shall be destroyed according to roles provided by the BSC (Board of Special Cases).

BUDAPEST CONVENTION DOMESTIC LEGISLATION Telecommunications Business Act B.E. 2544 (2001), Chapter V: Rights of service user Section 50 The Commission (National Telecommunications Commission) shall establish measures for user protection concerning personal data, right to privacy and freedom to communicate by means of telecommunications. The licensee shall have the duty to comply with the measures prescribed by the Commission under paragraph one. When it is found that there is a person who breaches the rights of a service user under paragraph one, the licensee or the Commission shall take action to terminate such breach and inform the user promptly. Article 16 - Expedited preservation of stored computer data CCA (2007, amended 2017) Chapter II: Competent officials 1 Each Party shall adopt such legislative and other measures as may be Section 26 necessary to enable its competent authorities to order or similarly obtain the A service provider is obliged to retain computer traffic data for at least ninety expeditious preservation of specified computer data, including traffic data, days from the date on which the data is entered into a computer system. If that has been stored by means of a computer system, in particular where necessary, on a particular provider and on a particular occasion, a competent there are grounds to believe that the computer data is particularly official may instruct a service provider to retain such computer traffic data for vulnerable to loss or modification. longer than ninety days but not exceeding two years. 2 Where a Party gives effect to paragraph 1 above by means of an order to a Criteria for computer traffic data storage of service providers (2007) person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
under Article 16, such legislative and other measures as may be necessary to:	Section 26 A service provider is obliged to retain computer traffic data for at least ninety days from the date on which the data is entered into a computer system. If necessary, on a particular provider and on a particular occasion, a competent official may instruct a service provider to retain such computer traffic data for longer than ninety days but not exceeding two years. Criteria for computer traffic data storage of service providers (2007)
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.	CCA (2007, amended 2017) Chapter II: Competent officials Section 18 With the enforcement of Section 19 and for the benefit of an investigation, when it could be reasonably believed that there is a perpetration of an offense under this Act, or there is a request per Paragraph Two, the competent official shall have one of the following powers necessary for the acquisition of evidence to prove the perpetration and to identify the perpetrators: (1) issue an inquiry letter or summon any person related to the perpetration of an offense to testify, to explain in letter, or to submit any other document, data, or evidence in the comprehensible form; (2) request computer traffic data, from a service provider related to communication via computer system, or from other related persons; (3) instruct a service provider to surrender user-related data that must be retained under Section 26, or that is in the service provider's possession or control, to a competent official, or to keep the data for later; (4) make a copy of computer data and computer traffic data from a computer system reasonably believed to have been used for the perpetration of an offense, if that computer system is not yet in the possession of the competent

DOMESTIC LEGISLATION

- 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.

official;

- (5) instruct a person, who is in possession or in control of computer data or a computer data storage device, to surrender the computer data or the device to the competent official;
- (6) inspect or access any person's computer system, computer data, computer traffic data, or computer data storage device, which is or can be used as evidence related to the perpetration of the offense; or which is for the identification of the perpetrator of the offense; and may instruct that person to surrender relevant computer data and computer traffic data to all necessary extent as well;
- (7) decrypt any person's computer data; or instruct any person related to the encryption of the computer data to decrypt the data, or to cooperate with a competent official in such decryption;
- (8) seize or forfeit a computer system as necessary for the benefit of obtaining details of the offense and the perpetrators of the offense.

For the benefit of the investigation and interrogation of the inquiry official per the Criminal Procedure Code, if there is a criminal offense against other laws which has made use of a computer system, computer data, or a computer storage device, as an accessory for the perpetration, or if there is computer data related to the perpetration of criminal offense against other laws, the inquiry official may request the competent official per Paragraph One to execute power per Paragraph One. Or if it dawns on the competent official as a result of the execution of duties per this Act, the competent official shall urgently compile facts and evidence and inform the relevant official for further action.

The person receiving the request from the competent official as to Paragraph One (1), (2), and (3) shall without delay act as requested, but not longer than seven days since the day the request was received; or act within the time specified by the competent official, which shall not less than seven days and not exceeding fifteen days. Except when there is a reasonable cause and with permission from the competent official. The Minister may publish in the Government Gazette prescribing the duration to carry out the request as appropriate to types of the service provider.

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

CCA (2007, amended 2017) **Chapter II: Competent officials**

Section 18

With the enforcement of Section 19 and for the benefit of an investigation, when

DOMESTIC LEGISLATION

access:

- a a computer system or part of it and computer data stored therein; and
- b a computer-data storage medium in which computer data may be stored

in its territory.

- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- a seize or similarly secure a computer system or part of it or a computer-data storage medium;
 - b make and retain a copy of those computer data:
 - c maintain the integrity of the relevant stored computer data;
 - d render inaccessible or remove those computer data in the accessed computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

it could be reasonably believed that there is a perpetration of an offense under this Act, or there is a request per Paragraph Two, the competent official shall have one of the following powers necessary for the acquisition of evidence to prove the perpetration and to identify the perpetrators:

- (1) issue an inquiry letter or summon any person related to the perpetration of an offense to testify, to explain in letter, or to submit any other document, data, or evidence in the comprehensible form;
- (2) request computer traffic data, from a service provider related to communication via computer system, or from other related persons;
- (3) instruct a service provider to surrender user-related data that must be retained under Section 26, or that is in the service provider's possession or control, to a competent official, or to keep the data for later;
- (4) make a copy of computer data and computer traffic data from a computer system reasonably believed to have been used for the perpetration of an offense, if that computer system is not yet in the possession of the competent official;
- (5) instruct a person, who is in possession or in control of computer data or a computer data storage device, to surrender the computer data or the device to the competent official;
- (6) inspect or access any person's computer system, computer data, computer traffic data, or computer data storage device, which is or can be used as evidence related to the perpetration of the offense; or which is for the identification of the perpetrator of the offense; and may instruct that person to surrender relevant computer data and computer traffic data to all necessary extent as well:
- (7) decrypt any person's computer data; or instruct any person related to the encryption of the computer data to decrypt the data, or to cooperate with a competent official in such decryption;
- (8) seize or forfeit a computer system as necessary for the benefit of obtaining details of the offense and the perpetrators of the offense.

For the benefit of the investigation and interrogation of the inquiry official per the Criminal Procedure Code, if there is a criminal offense against other laws which has made use of a computer system, computer data, or a computer storage device, as an accessory for the perpetration, or if there is computer data related to the perpetration of criminal offense against other laws, the inquiry official may request the competent official per Paragraph One to execute power

DOMESTIC LEGISLATION

per Paragraph One. Or if it dawns on the competent official as a result of the execution of duties per this Act, the competent official shall urgently compile facts and evidence and inform the relevant official for further action.

The person receiving the request from the competent official as to Paragraph One (1), (2), and (3) shall without delay act as requested, but not longer than seven days since the day the request was received; or act within the time specified by the competent official, which shall not less than seven days and not exceeding fifteen days. Except when there is a reasonable cause and with permission from the competent official. The Minister may publish in the Government Gazette prescribing the duration to carry out the request as appropriate to types of the service provider.

Section 19

In the exercise of power of the competent official under Section 18 (4), (5), (6), (7), and (8), the competent official shall file a petition to the court of jurisdiction for a court order to authorize the competent official to take action. The petition must identify a reasonable ground to believe that the person is perpetrating or going to perpetrate an offense, reasons for the exercise of such power, characteristics of the offense, description of the devices used for perpetrating the offense and of the alleged offender, as much as this can be identified. The court should adjudicate urgently such aforementioned petition.

When the court approves permission, and before taking any action according to the court order, the competent official shall submit a copy of the reasonable ground memorandum to show that an authorization under Section 18 (4), (5), (6), (7) and (8), must be employed against the owner or possessor of the computer system, as evidence thereof. If there is no owner of such computer thereby, the competent official should submit a copy of said memorandum as soon as possible.

In order to take action under Section 18 (4), (5), (6), (7) and (8), the senior officer of the competent official shall deliver a copy of the memorandum about the description and rationale of the operation to the court of jurisdiction within forty-eight (48) hours after the action has been taken as evidence thereof.

BUDAPEST CONVENTION DOMESTIC LEGISLATION When copying computer data under Section 18 (4), and given that it may be done only when there is a reasonable ground to believe that there is an offense against this Act, such action must not excessively interfere or obstruct the business operation of the computer data's owner or possessor. Regarding seizure or attachment under Section 18 (8), a competent official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. This is provided, however, that the seizure or attachment shall not last longer than thirty days. If seizure or attachment requires a longer time period, a petition shall be filed at the court of jurisdiction for the extension of the seizure or attachment time period. The court may allow only one or several time extensions, however altogether for no longer than sixty days. When that seizure or attachment is no longer necessary, or upon its expiry date, the competent official must immediately return the computer system that was seized or withdraw the attachment. The letter of seizure or attachment under Paragraph Five shall be in accordance with a Ministerial Regulation. Section 20 When there is an action to disseminate computer data as follows, the competent official, with approval from the Minister, may file a petition with supporting evidence, to the court of jurisdiction, for a court order to suppress the dissemination or to remove such computer data from a computer system. (1) Computer data actionable per this Act; (2) Computer data which may compromise the security of the Kingdom as prescribed in Book II Title 1 or Title 1/1 of the Criminal Code; (3) Computer data which is a criminal offense per laws related to intellectual property or other laws, where such computer data is a breach to the public order or moral high ground of the people, and the law enforcement official or the inquiry official per the Criminal Procedure Code has made a request about.

When there is an action to disseminate computer data which is appropriate to be a breach to the public order or moral high ground of the people, the Minister,

DOMESTIC LEGISLATION

with approval of the Computer Data Screening Committee, may authorize a competent official to file a petition with supporting evidence to the court of jurisdiction for a court order to suppress the dissemination or to remove such computer data from a computer system. The meeting of the Computer Data Screening Committee shall be governed by provisions on the committee authorized to carry out administrative procedure under the administrative procedure law mutatis mutandis.

The Minister shall appoint one or more of Computer Data Screening Committee per Paragraph Two. Each committee shall be consisted of nine members, three of whom must come from private sector in the fields of human rights, mass communication, information technology, or other relevant fields. The committee members shall be remunerated as per the criteria prescribed by the Minister with approval from the Ministry of Finance.

The act of the court per Paragraph One and Paragraph Two shall be guided by the Criminal Procedure Code mutatis mutandis. When the court issues an order to suppress the dissemination or to remove such computer data per Paragraph One or Paragraph Two, the competent official may suppress the dissemination or remove the computer data themselves or instruct the service provider to suppress the dissemination or remove the computer data. The Minister shall issue a Ministerial Notification prescribing the criteria, duration, and procedure to suppress the dissemination or to remove the computer data, for the competent official and the service provider, and they shall be made compatible to each other, with the consideration of the changing technological development, unless the court had instructed otherwise.

In case of necessity and emergency, the competent official may file the petition for the court order per Paragraph One before obtaining any approval from the Minister, and the competent official with approval from the Computer Data Screening Committee may file the petition for the court order per Paragraph Two before obtaining any authorization from the Minister, but it is obliged that they urgently bring the matter to the attention of the Minister.

CCA (2007, amended 2017) Chapter II: Competent officials

DOMESTIC LEGISLATION

Section 21

If a competent official found that any computer data contains undesirable set of instructions, the competent official may file a petition, to the court of jurisdiction, for a court order to prohibit the sale or the dissemination of that computer data; or to instruct the person who owns or possesses that computer data to suspend the use, destroy, or correct the computer data; or to impose a condition with respect to the use, possession, or dissemination of the undesirable set of instructions.

The undesirable set of instructions under Paragraph One shall refer to a set of instructions which causes a computer data, a computer system, or other sets of instructions to be damaged, destroyed, altered or appended, malfunction or failed to perform according to instructions, or otherwise as prescribed in Ministerial Regulations. The exception shall be made to an undesirable set of instructions that may be used for the prevention or the correction of the foregoing set of instructions. The Minister may publish in the Government Gazette, prescribing list of names, characteristics, or details of the undesirable set of instructions which can be used to prevent or correct the undesirable set of instructions.

Section 22

A competent official and an inquiry official in the case under Section 18 Paragraph Two shall not disclose or surrender computer data, computer traffic data, or user data, that acquired under Section 18, to any person.

The provisions under Paragraph One shall not apply to any action performed for the benefit of lodging a lawsuit against a perpetrator under this Act or a perpetrator under other laws in the case under Section 18 Paragraph Two; or for the benefit of lodging a lawsuit against a competent official on the grounds of their abuse of authority or against an inquiry official on the grounds of their abuse in the part that related to their duty under Section 18 Paragraph Two; or for action taken according to a court order or permission.

Any competent official or inquiry official who violates Paragraph One must be subject to imprisonment not exceeding three years or a fine not exceeding sixty

DOMESTIC LEGISLATION

Article 20 - Real-time collection of traffic data

- Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
 - collect or record through the application of technical means on the territory of that Party, and
- 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
 - to co-operate and assist the competent authorities in the or evidence in the comprehensible form; ii collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
- 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.
- 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.
- The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

thousand baht, or both. CCA (2007, amended 2017) Chapter II: Competent officials

Section 18

With the enforcement of Section 19 and for the benefit of an investigation, when it could be reasonably believed that there is a perpetration of an offense under this Act, or there is a request per Paragraph Two, the competent official shall have one of the following powers necessary for the acquisition of evidence to prove the perpetration and to identify the perpetrators:

- (1) issue an inquiry letter or summon any person related to the perpetration of an offense to testify, to explain in letter, or to submit any other document, data,
- (2) request computer traffic data, from a service provider related to communication via computer system, or from other related persons;
- (3) instruct a service provider to surrender user-related data that must be retained under Section 26, or that is in the service provider's possession or control, to a competent official, or to keep the data for later;
- (4) make a copy of computer data and computer traffic data from a computer system reasonably believed to have been used for the perpetration of an offense, if that computer system is not yet in the possession of the competent official:
- (5) instruct a person, who is in possession or in control of computer data or a computer data storage device, to surrender the computer data or the device to the competent official;
- (6) inspect or access any person's computer system, computer data, computer traffic data, or computer data storage device, which is or can be used as evidence related to the perpetration of the offense; or which is for the identification of the perpetrator of the offense; and may instruct that person to surrender relevant computer data and computer traffic data to all necessary extent as well;
- (7) decrypt any person's computer data; or instruct any person related to the encryption of the computer data to decrypt the data, or to cooperate with a competent official in such decryption;
- (8) seize or forfeit a computer system as necessary for the benefit of obtaining details of the offense and the perpetrators of the offense.

For the benefit of the investigation and interrogation of the inquiry official per the Criminal Procedure Code, if there is a criminal offense against other laws

DOMESTIC LEGISLATION

which has made use of a computer system, computer data, or a computer storage device, as an accessory for the perpetration, or if there is computer data related to the perpetration of criminal offense against other laws, the inquiry official may request the competent official per Paragraph One to execute power per Paragraph One. Or if it dawns on the competent official as a result of the execution of duties per this Act, the competent official shall urgently compile facts and evidence and inform the relevant official for further action.

The person receiving the request from the competent official as to Paragraph One (1), (2), and (3) shall without delay act as requested, but not longer than seven days since the day the request was received; or act within the time specified by the competent official, which shall not less than seven days and not exceeding fifteen days. Except when there is a reasonable cause and with permission from the competent official. The Minister may publish in the Government Gazette prescribing the duration to carry out the request as appropriate to types of the service provider.

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:

ito 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 official;

<u>Criteria for computer traffic data storage of service providers</u> (2007)

CCA (2007, amended 2017) Chapter II: Competent officials

Section 18

With the enforcement of Section 19 and for the benefit of an investigation, when it could be reasonably believed that there is a perpetration of an offense under this Act, or there is a request per Paragraph Two, the competent official shall have one of the following powers necessary for the acquisition of evidence to prove the perpetration and to identify the perpetrators:

- (1) issue an inquiry letter or summon any person related to the perpetration of an offense to testify, to explain in letter, or to submit any other document, data, or evidence in the comprehensible form;
- (2) request computer traffic data, from a service provider related to communication via computer system, or from other related persons;
- (3) instruct a service provider to surrender user-related data that must be retained under Section 26, or that is in the service provider's possession or control, to a competent official, or to keep the data for later;
- (4) make a copy of computer data and computer traffic data from a computer system reasonably believed to have been used for the perpetration of an offense, if that computer system is not yet in the possession of the competent official:

DOMESTIC LEGISLATION

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.

- (5) instruct a person, who is in possession or in control of computer data or a computer data storage device, to surrender the computer data or the device to the competent official:
- (6) inspect or access any person's computer system, computer data, computer traffic data, or computer data storage device, which is or can be used as evidence related to the perpetration of the offense; or which is for the identification of the perpetrator of the offense; and may instruct that person to surrender relevant computer data and computer traffic data to all necessary extent as well:
- (7) decrypt any person's computer data; or instruct any person related to the encryption of the computer data to decrypt the data, or to cooperate with a competent official in such decryption:
- (8) seize or forfeit a computer system as necessary for the benefit of obtaining details of the offense and the perpetrators of the offense.

For the benefit of the investigation and interrogation of the inquiry official per the Criminal Procedure Code, if there is a criminal offense against other laws which has made use of a computer system, computer data, or a computer storage device, as an accessory for the perpetration, or if there is computer data related to the perpetration of criminal offense against other laws, the inquiry official may request the competent official per Paragraph One to execute power per Paragraph One. Or if it dawns on the competent official as a result of the execution of duties per this Act, the competent official shall urgently compile facts and evidence and inform the relevant official for further action.

The person receiving the request from the competent official as to Paragraph One (1), (2), and (3) shall without delay act as requested, but not longer than seven days since the day the request was received; or act within the time specified by the competent official, which shall not less than seven days and not exceeding fifteen days. Except when there is a reasonable cause and with permission from the competent official. The Minister may publish in the Government Gazette prescribing the duration to carry out the request as appropriate to types of the service provider.

Section 3 - Jurisdiction

Article 22 - Jurisdiction

Each Party shall adopt such legislative and other measures as may be Section 19

CCA (2007, amended 2017) Chapter II: Competent officials

DOMESTIC LEGISLATION

necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

- a in its territory; or
- b on board a ship flying the flag of that Party; or
- c on board an aircraft registered under the laws of that Party; or
- d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
- 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.
- 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

In the exercise of power of the competent official under Section 18 (4), (5), (6), (7), and (8), the competent official shall file a petition to the court of jurisdiction for a court order to authorize the competent official to take action. The petition must identify a reasonable ground to believe that the person is perpetrating or going to perpetrate an offense, reasons for the exercise of such power, characteristics of the offense, description of the devices used for perpetrating the offense and of the alleged offender, as much as this can be identified. The court should adjudicate urgently such aforementioned petition.

When the court approves permission, and before taking any action according to the court order, the competent official shall submit a copy of the reasonable ground memorandum to show that an authorization under Section 18 (4), (5), (6), (7) and (8), must be employed against the owner or possessor of the computer system, as evidence thereof. If there is no owner of such computer thereby, the competent official should submit a copy of said memorandum as soon as possible.

In order to take action under Section 18 (4), (5), (6), (7) and (8), the senior officer of the competent official shall deliver a copy of the memorandum about the description and rationale of the operation to the court of jurisdiction within forty-eight (48) hours after the action has been taken as evidence thereof.

When copying computer data under Section 18 (4), and given that it may be done only when there is a reasonable ground to believe that there is an offense against this Act, such action must not excessively interfere or obstruct the business operation of the computer data's owner or possessor.

Regarding seizure or attachment under Section 18 (8), a competent official must issue a letter of seizure or attachment to the person who owns or possesses that computer system as evidence. This is provided, however, that the seizure or attachment shall not last longer than thirty days. If seizure or attachment requires a longer time period, a petition shall be filed at the court of jurisdiction for the extension of the seizure or attachment time period. The court may allow only one or several time extensions, however altogether for no longer than sixty days. When that seizure or attachment is no longer necessary, or upon its

BUDAPEST CONVENTION DOMESTIC LEGISLATION

expiry date, the competent official must immediately return the computer system that was seized or withdraw the attachment.

The letter of seizure or attachment under Paragraph Five shall be in accordance with a Ministerial Regulation.

CCA (2007, amended 2017) **Chapter II: Competent officials**

Section 20

When there is an action to disseminate computer data as follows, the competent official, with approval from the Minister, may file a petition with supporting evidence, to the court of jurisdiction, for a court order to suppress the dissemination or to remove such computer data from a computer system.

- (1) Computer data actionable per this Act;
- (2) Computer data which may compromise the security of the Kingdom as prescribed in Book II Title 1 or Title 1/1 of the Criminal Code;
- (3) Computer data which is a criminal offense per laws related to intellectual property or other laws, where such computer data is a breach to the public order or moral high ground of the people, and the law enforcement official or the inquiry official per the Criminal Procedure Code has made a request about.

When there is an action to disseminate computer data which is appropriate to be a breach to the public order or moral high ground of the people, the Minister, with approval of the Computer Data Screening Committee, may authorize a competent official to file a petition with supporting evidence to the court of jurisdiction for a court order to suppress the dissemination or to remove such computer data from a computer system. The meeting of the Computer Data Screening Committee shall be governed by provisions on the committee authorized to carry out administrative procedure under the administrative procedure law mutatis mutandis.

The Minister shall appoint one or more of Computer Data Screening Committee per Paragraph Two. Each committee shall be consisted of nine members, three of whom must come from private sector in the fields of human rights, mass communication, information technology, or other relevant fields. The committee members shall be remunerated as per the criteria prescribed by the Minister

BUDAPEST CONVENTION DOMESTIC LEGISLATION with approval from the Ministry of Finance. The act of the court per Paragraph One and Paragraph Two shall be guided by the Criminal Procedure Code mutatis mutandis. When the court issues an order to suppress the dissemination or to remove such computer data per Paragraph One or Paragraph Two, the competent official may suppress the dissemination or remove the computer data themselves or instruct the service provider to suppress the dissemination or remove the computer data. The Minister shall issue a Ministerial Notification prescribing the criteria, duration, and procedure to suppress the dissemination or to remove the computer data, for the competent official and the service provider, and they shall be made compatible to each other, with the consideration of the changing technological development, unless the court had instructed otherwise. In case of necessity and emergency, the competent official may file the petition for the court order per Paragraph One before obtaining any approval from the Minister, and the competent official with approval from the Computer Data Screening Committee may file the petition for the court order per Paragraph

CCA (2007, amended 2017) Chapter II: Competent officials Section 21

they urgently bring the matter to the attention of the Minister.

If a competent official found that any computer data contains undesirable set of instructions, the competent official may file a petition, to the court of jurisdiction, for a court order to prohibit the sale or the dissemination of that computer data; or to instruct the person who owns or possesses that computer data to suspend the use, destroy, or correct the computer data; or to impose a condition with respect to the use, possession, or dissemination of the undesirable set of instructions.

Two before obtaining any authorization from the Minister, but it is obliged that

The undesirable set of instructions under Paragraph One shall refer to a set of instructions which causes a computer data, a computer system, or other sets of instructions to be damaged, destroyed, altered or appended, malfunction or failed to perform according to instructions, or otherwise as prescribed in

DOMESTIC LEGISLATION

Ministerial Regulations. The exception shall be made to an undesirable set of instructions that may be used for the prevention or the correction of the foregoing set of instructions. The Minister may publish in the Government Gazette, prescribing list of names, characteristics, or details of the undesirable set of instructions which can be used to prevent or correct the undesirable set of instructions.

<u>Thailand Criminal Code B.E. 2499</u> (1956), Book I, Title I: Provisions applicable to general offences, Chapter 2: Application of criminal laws Section 4

Whoever, committing an offence within the Kingdom, shall be punished according to law.

The offence committed in any Thai vessel or airplane irrespective of any place of Thai vessel or airplane shall be deemed as being committed within the Kingdom.

Section 5

Whenever any offence is even partially committed within the Kingdom, or the consequence of the commission of which, as intended by the offender, occurs within the Kingdom, or by the nature of the commission of which, the consequence resulting therefrom should occur within the Kingdom, or it could be foreseen that the consequence would occur within the Kingdom, it shall be deemed that such offence is committed within the Kingdom.

In case of preparation or attempt to commit any act provided by the law to be an offence, even though it is done outside the Kingdom, if the consequence of the doing of such act, when carried through to the stage of accomplishment of the offence, will occur within the Kingdom, it shall be deemed that the preparation or attempt to commit such offence is done within the Kingdom.

Section 6

Any offence has been committed within the Kingdom, or has been deemed by this Code as being committed within the Kingdom, even though the act of a coprincipal, a supporter or an instigator of the offence has been committed outside the Kingdom it shall be deemed that the principal, supporter or instigator has committed the offence within the Kingdom.

BUDAPEST CONVENTION DOMESTIC LEGISLATION Section 7 Whoever commits the following offences outside the Kingdom shall be punished in the Kingdom, namely: (1) Offences Relating to the Security of the Kingdom as provided in Sections 107 to 129: (1/1) The offence of terrorization as prescribed by Section 135/1, Section 135/2, Section 135/3 and Section 135/4; (2) Offences Relating to Counterfeiting and Alternation as provided in Section 240 to Section 249, Section 254, Section 256, Section 257 and Section 266(3) and (4); (2bis) Offences relating to sexuality as provided in Section 282 and Section 283; (3) Offence Relating to Robbery as provided in Section 339, and offences relating to gang-robbery as provided in Section 340, which is committed on the high seas. Section 8 Whoever commits an offence outside the Kingdom shall be punished in the Kingdom; provided that, and, provided further that the offence committed be any of the following namely: (a) The offender be a Thai person, and there be a request for punishment by the Government of the country where the offence has occurred or by the injured person; or (b) The offender be an alien, and the Thai Government or a Thai person be the injured person, and there be a request for punishment by the injured person. If such offence to be the offence specified as following shall be punished within the Kingdom namely: (1) Offence Relating to Cause Public Dangers as provided in Section 217, Section 218, Section 221 to Section 223 excepting the case relating to the first paragraph of Section 220, and Section 224, Section 226, Section 228 to Section 232, Section 237, and Section 233 to Section 236 only when it is the case to be punished according to Section 238; (2) Offences Relating to Documents as provided in Section 264, Section 265,

and Section 269;

Section 266(1) and (2), Section 268 excepting the case relating to Section 267

BUDAPEST CONVENTION DOMESTIC LEGISLATION (2/1) Offences Relating to the Electronic Card according to be prescribed by Section 269/1 to Section 269/7. (3) Offences Relating to Sexuality as provided in Section 276, Section 280 and Section 285 only for the case relating to Section 276; (4) Offences Against Life as provided in Section 288 to Section 290; (5) Offences Against Body as provided in Section 295 to Section 298; (6) Offences of Abandonment of Children, Sick or Aged Persons as provided in Section 306 to Section 308; (7) Offences Against Liberty as provided in Section 309, section 310, Section 312 to Section 315, and Section 317 to Section 320; (8) Offences of Theft and Snatching as provided in Section 334 to Section 336; (9) Offences of Extortion, Blackmail, Robbery and Gang-Robbery as provided in Section 337 to Section 340; (10) Offences of Cheating and Fraud as provided in Section 341 to Section 344, Section 346 and Section 347; (11) Offences of Criminal Misappropriation as provided in Section 352 to Section 354: (12) Offences of Receiving Stolen Property as provided in Section 357; (13) Offences of Mischief as provided in Section 358 to section 360. Section 9 Thai Government official commits the offence as prescribed from Section 147 to Section 166 and from Section 200 to Section 205 outside the Kingdom shall be punished in the Kingdom. Section 10 Whoever does an act outside the Kingdom, which is an offence according to various Sections as specified in Section 7(2) and (3), Section 8 and Section 9 shall not be punished again in the Kingdom for the doing of such act, if: (1) They received a final foreign Court decision to be released; or (2) The foreign Court sentenced the offender to be punished but was later acquitted. If the offender was punished for such action in accordance with the judgment of

the foreign Court and has already executed their punishment and was not

BUDAPEST CONVENTION DOMESTIC LEGISLATION acquitted, the Thai Court - taking into consideration the sentence that person has already served, can punish less than the law requires for that offense or give no punishment at all. Section 11 Whoever commits an offence within the Kingdom, or commits an offence deemed by this Code as being committed within the Kingdom, and, if such person has suffered the punishment in whole or in part for such act according to the judgement of the foreign Court, the Court may inflict less punishment to any extent than that provided by the law for such offence, or may not inflict any punishment at all, by having regard to the punishment already suffered by such person. In case of a person, committing an offence within the Kingdom, or committing an offence deemed by this Code as being committed within the Kingdom, has been prosecuted in the foreign Court at the request of the Thai government, such person shall not be punished again in the Kingdom for such offence, if: (1) There be a final judgement of the foreign Court acquitting such person; or (2) There be a judgement of the foreign Court convicting such person, and such person has already executed their punishment. Section 17 The provisions of Book 1 of this Code shall be used in case of offenses according to other laws too, unless those laws prescribe otherwise.

Criminal Procedure Code B.E. 2477 (1934) as amended to Act No. 28 of 2551 (2008), Title II: Powers of inquiry officials and competency of courts, Chapter I: General provisions

Section 16

The jurisdiction of Courts and the competency of judges, Public Prosecutors and administrative or police officials for the execution of the provisions of this Code shall be governed by the laws and rules concerning the organization of Courts and the powers and duties of judges, or concerning Public Prosecutors and administrative of police officials respectively.

BUDAPEST CONVENTION DOMESTIC LEGISLATION Act Amending the Code of Criminal Procedure (No. 29) B.E. 2551 (2008) Section 20 Where an offence punishable under Thai law is committed outside the Kingdom of Thailand, the Attorney General or his substitute shall be responsible for an inquiry into such offence. But he may authorize any public prosecutor or judicial police officer to conduct that inquiry on his behalf. In cases the Attorney General or his substitute authorizes any judicial police officer take charge of the inquiry; he may also authorize any public prosecutor to take part therein with the judicial police officer. The public prosecutor authorized to carry out or take part in the inquiry shall assume the same authority as a judicial police officer and all other authority bestowed on him by the legal provisions. If a public prosecutor takes part in an inquiry with a judicial police officer, the latter shall adhere to the orders and instructions given by the former in respect of the collection of evidence. In case of need, the following judicial police officers shall be permitted to hold an inquiry pending any order of the Attorney General or his substitute: (1) The judicial police officer in whose territorial jurisdiction the accused is arrested; (2) The judicial police officer requested by the foreign government or victim to prosecute the accused. Finding that the inquiry is completed, the public prosecutor or judicial police officer responsible therefore, as the case may be, shall make an opinion pursuant to Section 140, Section 141 or Section 142 and submit it together with the file to the Attorney General or his substitute. Criminal Procedure Code B.E. 2477 (1934) as amended to Act No. 28 of 2551 (2008), Title II: Powers of inquiry officials and competency of courts, Chapter III: Competency of Courts Section 22 When an offence has been committed, alluded or believed to have been committed within the territorial jurisdiction of any Court, it shall be tried and

adjudicated by such Court. [...]

DOMESTIC LEGISLATION

(2) Where the offence has been committed outside Thailand, it shall be tried and adjudicated by the Criminal Court. If the inquiry has been conducted in a locality situated within the territorial jurisdiction of any Court, the case may also be tried and adjudicated by such Court.

Regulations of Ministry of Interior Issued under Section 5 of Act Promulgating the Criminal Procedure Code B.E. 2477

- 1. If the offence punishable under Thai law has been committed outside Thailand and apt to be investigated under "the Criminal Procedure Code", inquiry official whom alleged offender has been arrested territorial jurisdiction or inquiry official which other government of country or injured person has sued to convict alleged offender, shall notify "Director-General of the Public Prosecution Department" or "person in charge", and if the notice through the writings is delayed, it shall be notified through telegraph and in the writings or telegraph at the least specified, as follows:
- (1) Name and nationality of alleged offender;
- (2) Accused as committed in which count or where;
- (3) Name and nationality of injured person, if any;
- (4) Alleged offender arrested yet? Where? When?

In case of "the Director-General of the Public Prosecution Department" or "the person in charge of one's functions" has issued an order delegating such duty to any inquiry official conducting an inquiry and when the inquiry has been proceeded, if "the Director-General of the Public Prosecution Department" or "the person in charge of one's functions" has not issued an order otherwise, the inquiry official shall file of the inquiry to public prosecutor in the locality where inquiry has proceeded for executing under the powers and duties.

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.

Extradition Act B.E. 2551 (2008)

- > Chapter 1: General extradition principles
- > Chapter 2: Initiating proceedings upon request
 - Part 1: General provisions
 - Part 2: Extradition procedures
 - Part 3: Appeal
- > Chapter 3: Extradition

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

DOMESTIC LEGISLATION

- > Chapter 4: Requests for extradition made by Thailand
- > Chapter 5: Extradition expenses; Transitory provisions

Most provisions but especially:

Section 4

This Act shall be applicable to all extradition proceedings so far as it is not inconsistent with the terms of any extradition treaty between the Government of Thailand and foreign government or international organization.

Chapter 1: General Extradition Principles Section 7

An extraditable offense shall be criminal and punishable under the laws of Requesting State and Thailand by death penalty, imprisonment, deprivation of liberty, or other detention forms for a period of more than one year, to an offense of the same Chapter or same offense in both states.

Other criminal offense punishable by imprisonment, deprivation of liberty or other detention forms less than one year shall also be an extraditable, if it is an extraditable offense as requested, whether it is requested for the first time or subsequently requested.

Section 8

Extradition proceedings shall commence with a request from Requesting State. The state having extradition treaty with Thailand shall submit its request for extradition to the Central Authority. The state that has no such treaty shall submit its request through the diplomatic channel.

A request for extradition and supporting documents shall conform to the regulations, means and conditions prescribed by the Ministerial Regulations.

A request for extradition and supporting documents described in paragraph 3 to be submitted to the court shall be translated into Thai and its correctness shall be certified.

A request for extradition or supporting documents under this Chapter shall also be submitted to the court without witnesses.

DOMESTIC LEGISLATION

updated a register of authorities so designated by the Parties. Each Party shall ensure

Section 9

The Government of Thailand may consider the extradition for legal proceedings or conviction according to the judgement in criminal offense within the jurisdiction of Requesting State as requested in the following cases:

- (1) If it is an extraditable offense and it is not forbidden under Thai law or it is not the military or political offense.
- (2) If there exists no mutual treaty and the Requesting State commits to assist Thailand in the similar manner when requested.

The political offense described in paragraph 1 does not include the following offense:

- (1) Assassination, attack or liberty deprivation of the king, queen or heir to the throne.
- (2) Assassination, physical attack or liberty deprivation of chief of the state, government leader or his/her member.
- (3) Offense which is not considered to be a political offense for extradition purpose under Treaty which Thailand is a contracting party.

Military offense means an exclusive military offense, not criminal offense in general.

Section 10

If a person whom the extradition is requested has previously been judged by the court of Thailand or the court of Requesting State in the same act, and according to the final judgement, the person has been released or convicted and the person has been out of penalty or has received a general pardon or amnesty, or the prescription in law has been expired, or under any circumstances, the person has not been charged by the law of Requesting State, the person shall not be extradited from such act again.

Section 11

A person extradited may not be detained, tried, or punished in the Requesting State except for any offense for which extradition was granted, nor be extradited by the State to a third state, unless:

- (1) that person has left the territory of the Requesting State after extradition and has voluntarily returned to it.
- (2) that person has not left the territory of the Requesting State within 45 days

BUDAPEST CONVENTION DOMESTIC LEGISLATION after being free to do so, or (3) the Requested State has agreed. Chapter 3: Extradition Section 22 After the final judgment has been given to detain the person sought and the Government of Thailand has approved the extradition, the surrender of person sought to the Requesting State shall be done within ninety days from the date of final judgment or within such extended time as the Court permits as requested by the public prosecutor. The date, time, place and method of surrender for extradition shall conform to the Ministerial Regulations. Section 23 If the Requesting State fails to take the surrender of person sought for extradition within a period prescribed under Section 22 without a reasonable ground, the Requested State may subsequently refuse extradition for the same offense(s). The refusal of extradition defined in paragraph 1 shall not be subject to the provisions of Section 25. Section 24 If the person under the final judgment of detention for extradition is charged or

(1) To surrender the person to the Requesting State.

of the following procedures:

(2) To postpone the surrender until the litigation ends or until the person serves some or whole prison term according to the judgment.

is imprisoned according to the judgment in Thailand for offense(s) other than offense(s) committed for extradition, the Government of Thailand may take any

(3) To surrender the person to the Requesting State on temporary basis for litigation under conditions agreed by the Requesting State, and after the person has been surrendered to Thailand, the person may be surrendered to the Requesting State again for penalty according to the judgment.

Section 25

If there is no extradition to the Requesting State, the Central Authority shall notify the Competent Authorities for criminal prosecution against the person

BUDAPEST CONVENTION DOMESTIC LEGISLATION sought for extradition under Thai law. Section 26 Unless otherwise considered by the cabinet, if the Requested State receives requests from two or more States for the extradition of the same person, either for the same offense or for different offenses, the Central Authority of the Requested State shall determine to which State and under what conditions it will surrender the person first. In making its decision, the Requested State shall consider all relevant factors: (1) whether or not the Requesting State has an extradition treaty with Thailand. (2) the place where each offense was committed. (3) the severity of offense which affects Requesting State and penalty (4) the order of request received from Requesting State (5) the nationality of the offender (6) the interest and readiness of prosecution (7) other reasons with respect to international relation according to the opinion given by the Ministry of Foreign Affairs. The Central Authority shall consider and notify the Requesting State and follow the procedures under this Act. Section 27 Upon the arrest of person sought, whether or not the request is made under this act, the Competent Authority shall ask the person of his/her consent for extradition. If the person sought in paragraph 1 expresses consent for extradition, it shall be made in writing in the form prescribed by the Central Authority, and the public prosecutor shall take the person to the court to file a petition for the court to examine the consent immediately. If the court finds that the person voluntarily gives consent, the court shall issue an order of detention for extradition under Section 22. The consent made before the court shall not be irrevocable. During the examination of the court, if the person changes mind on the consent expressed to the Competent Authority, the court shall issue an order of

detention for extradition consideration as prescribed under Chapter 2, Part 2.

DOMESTIC LEGISLATION

Section 28

If the extradition case is in the course of proceeding at any court and the person expresses consent before the court for extradition, the trial proceeding at the court shall not be required and the order of detention for extradition shall be issued under Section 22.

The consent made before the court shall not be irrevocable.

Deportation Act B.E. 2499 (1956) as amended until Act (No. 3) B.E. 2521 (1978)

Article 25 - General principles relating to mutual assistance

- 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
- 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
- 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
- 4 Except as otherwise specifically provided in articles in this chapter, mutual | Chapter 1: Central Authority assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the The Central Authority shall have the following authority and functions: 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 Royal Thai Government and deliver to the Requested State; offence.
- 5 Where, in accordance with the provisions of this chapter, the requested

Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992)

- **Chapter 1: Central Authority**
- > Chapter 2: Providing of and seeking for assistance
 - Part 1: General provisions
 - Part 2: Inquiry and producing evidence
 - Part 3: Providing of documents and information in the possession of government agencies
 - Part 4: Serving documents
 - Part 5: Search and seizure
 - Part 6: Transferring persons in custody for testimonial purposes
 - Part 7: Locating persons
 - Part 8: Initiating proceedings upon request
 - Part 9: Forfeiture or seizure of properties
 - Part 10: Seeking assistance
- > Chapter 3: Costs

Section 7

- (1) To receiving the request for assistance from the Requesting State and transmit it to the Competent Authorities;
- (2) To receive the request seeking assistance presented by the agency of the
- (3) To consider and determine whether to provide or seek assistance;
- (4) To follow and expedite the performance of the Competent Authorities in providing assistance to a foreign state for the purpose of expeditious conclusion;
- Party is permitted to make mutual assistance conditional upon the existence (5) To issue regulations or announcement for the implementation of this Act;

DOMESTIC LEGISLATION

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.

(6) To carry out other acts necessary for the success of providing or seeking assistance under this Act.

Ministerial Regulation B.E. 2537 (1994) issued under the Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992):

- > Chapter 1: Transferring of persons in custody in Thailand to testify in the requesting state
- > Chapter 2: Admission of persons in custody in the requesting state to testify in Thailand
- > Chapter 3: Miscellaneous

Article 26 - Spontaneous information

- 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
- 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

CCA (2007, amended 2017) **Chapter II: Competent officials**

Section 18

With the enforcement of Section 19 and for the benefit of an investigation, when it could be reasonably believed that there is a perpetration of an offense under this Act, or there is a request per Paragraph Two, the competent official shall have one of the following powers necessary for the acquisition of evidence to prove the perpetration and to identify the perpetrators:

- (1) issue an inquiry letter or summon any person related to the perpetration of an offense to testify, to explain in letter, or to submit any other document, data, or evidence in the comprehensible form;
- (2) request computer traffic data, from a service provider related to communication via computer system, or from other related persons;
- (3) instruct a service provider to surrender user-related data that must be retained under Section 26, or that is in the service provider's possession or control, to a competent official, or to keep the data for later;
- (4) make a copy of computer data and computer traffic data from a computer system reasonably believed to have been used for the perpetration of an offense, if that computer system is not yet in the possession of the competent official:
- (5) instruct a person, who is in possession or in control of computer data or a computer data storage device, to surrender the computer data or the device to the competent official;
- (6) inspect or access any person's computer system, computer data, computer traffic data, or computer data storage device, which is or can be used as evidence related to the perpetration of the offense; or which is for the identification of the perpetrator of the offense; and may instruct that person to surrender relevant computer data and computer traffic data to all necessary

BUDAPEST CONVENTION DOMESTIC LEGISLATION extent as well; (7) decrypt any person's computer data; or instruct any person related to the encryption of the computer data to decrypt the data, or to cooperate with a competent official in such decryption; (8) seize or forfeit a computer system as necessary for the benefit of obtaining details of the offense and the perpetrators of the offense. For the benefit of the investigation and interrogation of the inquiry official per the Criminal Procedure Code, if there is a criminal offense against other laws which has made use of a computer system, computer data, or a computer storage device, as an accessory for the perpetration, or if there is computer data related to the perpetration of criminal offense against other laws, the inquiry official may request the competent official per Paragraph One to execute power per Paragraph One. Or if it dawns on the competent official as a result of the execution of duties per this Act, the competent official shall urgently compile facts and evidence and inform the relevant official for further action. The person receiving the request from the competent official as to Paragraph One (1), (2), and (3) shall without delay act as requested, but not longer than seven days since the day the request was received; or act within the time specified by the competent official, which shall not less than seven days and not exceeding fifteen days. Except when there is a reasonable cause and with permission from the competent official. The Minister may publish in the Government Gazette prescribing the duration to carry out the request as appropriate to types of the service provider. Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992), Chapter 2: Providing of and seeking for assistance Part 3: Providing of documents and information in the possession of government agencies Section 19 If the documents or information sought under Section 18 should not be published and the agency maintaining such documents or information considers it impossible to disclose or should not disclose the said documents or

information, or possible to disclose them under certain conditions, the said agency shall acknowledge the Central Authority the causes of impossibility or

DOMESTIC LEGISLATION

the conditions required for the disclosure of such documents or information.

Part 10: Seeking assistance Section 39

The requesting agency shall comply the commitment of Thailand towards the Requested State regarding the use of information or evidence for the purpose specified in the request.

The requesting agency shall also comply with the commitment of Thailand towards the Requested State regarding the confidentiality of the requested information or evidence unless such information or evidence is necessary for the public trial, which is the consequence of the investigation, inquiry, prosecution or other criminal proceeding referred to in the request.

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 **Section 10** 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 | Section 11 for their execution.
- The central authorities shall communicate directly with each other;
- 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;
- 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.
- 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.

Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992), Chapter 2: Providing of and seeking for assistance, Part 1: General provisions

The state having a mutual assistance treaty with Thailand shall submit its request for assistance directly to the Central Authority. The state, which has no such treaty, shall submit its request through diplomatic channel.

A request for assistance shall conform to the forms, regulations, means and conditions defined by the Central Authority.

Upon receipt a request for assistance from a foreign state, the Central Authority shall consider and determine whether such request is eligible for the providing of assistance under this Act and has followed the process correctly as well as accompanied by all appropriate supporting documents.

If such request eligible for the providing of assistance, and in line with the process, as well as accompanied by all appropriate supporting documents, the Central Authority shall transmit the said request to the Competent Authorities for further execution.

If such request if not eligible for the providing of assistance, or must be subject to some essential conditions before the assistance is provided, or if it is not in line with the process or has not been accompanied by all appropriate supporting

DOMESTIC LEGISLATION

- The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
- the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
- it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.
- The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
- 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.
- 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.
- 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.
- 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.
- Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
- 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.
- involve coercive action may be directly transmitted by the competent Authorities shall report to the Central Authority the causes thereof.

documents required, the Central Authority shall refuse to provide assistance and notify the Requesting State the reasons thereof, or indicate the required conditions, or the causes of impossibility to execute the request.

If the Central Authority is of the view that the execution of a request may interfere with the investigation, inquiry, prosecution, or other criminal proceeding pending its handling in Thailand, he may postpone the execution of the said request or may execute it under certain conditions set by him and notify the Requesting State about that. A determination of the Central Authority with regard to the providing of assistance shall be final, unless otherwise alliterated by the Prime Minister.

Section 12

The requested Party shall promptly inform the requesting Party of the The Central Authority shall transmit the request for assistance from a foreign state to the following Competent Authorities for execution:

- (1) The request for taking statement of persons, or providing documents, articles, and evidence out of Court, the request for serving documents, the request for searches, the request for seizures documents or articles, and the request for locating persons shall be transmitted to the Director General of the Police Department:
- (2) The request for taking the testimony of persons and witnesses or adducing document and evidence in the Court, as well as the request for forfeiture or seizure of properties shall be transmitted to the Chief Public Prosecutor for Litigation:
- (3) The request for transferring persons in custody for testimonial purposes shall be transmitted to the Director General of the Correctional Department.
- (4) The request for initiating criminal proceedings shall be transmitted to the Director General of the Police Department and the Chief Public Prosecutor for Litigation.

Section 13

Upon receipt a request for assistance from the Central Authority, the Competent Authorities shall execute such request and, after completion, submit a report together with all documents and articles concerned to the Central Authority.

Requests or communications made under this paragraph that do not In cases of impediment or impossibility to execute the request, the Competent

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	Section 14 When the Competent Authorities finished the execution of a request and have already reported to the Central Authority, the Central Authority shall notify the result thereof as well as deliver all documents and articles concerned to the
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:	Part 3: Providing of documents and information in the possession of government agencies Section 19 If the documents or information sought under Section 18 should not be published and the agency maintaining such documents or information considers it impossible to disclose or should not disclose the said documents or information, or possible to disclose them under certain conditions, the said agency shall acknowledge the Central Authority the causes of impossibility or
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.	Section 39 The requesting agency shall comply the commitment of Thailand towards the Requested State regarding the use of information or evidence for the purpose specified in the request.
Article 29 – Expedited preservation of stored computer data 1 A Party may request another Party to order or otherwise obtain the	Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992)

located within the territory of that other Party and in respect of which the The Central Authority shall have the following authority and functions:

requesting Party intends to submit a request for mutual assistance for the (1) To receiving the request for assistance from the Requesting State and

expeditious preservation of data stored by means of a computer system, Section 7

DOMESTIC LEGISLATION

search or similar access, seizure or similar securing, or disclosure of the data.

- 2 A request for preservation made under paragraph 1 shall specify:
 - a the authority seeking the preservation;
- b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
- c the stored computer data to be preserved and its relationship to the offence:
- d any available information identifying the custodian of the stored computer data or the location of the computer system;
 - e the necessity of the preservation; and
- f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
- 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.
- 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.
- 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

transmit it to the Competent Authorities;

- (2) To receive the request seeking assistance presented by the agency of the Royal Thai Government and deliver to the Requested State;
- (3) To consider and determine whether to provide or seek assistance;
- (4) To follow and expedite the performance of the Competent Authorities in providing assistance to a foreign state for the purpose of expeditious conclusion;
- (5) To issue regulations or announcement for the implementation of this Act;
- (6) To carry out other acts necessary for the success of providing or seeking assistance under this Act.

<u>Treaty between Thailand and Canada on Mutual Assistance in Criminal</u> <u>Matters</u> (1994)

Article 5: Contents of requests for mutual assistance

- 1. A request for assistance shall be submitted in writing. In urgent circumstances or where otherwise permitted by the Requested State, a request may be made by facsimile but shall be confirmed in writing promptly thereafter.
- 2. All requests shall include the following:
- a) the name of the competent authority conducting the investigation, prosecution or proceeding to which the request relates;
- b) a description of the nature of the investigation, prosecution or proceeding, including a summary of the relevant facts and laws;
- c) a description of the evidence or information sought or the acts of assistance to be performed; and
- d) the purpose for which the evidence, information, or other assistance is sought.
- 3. When appropriate, a request shall also include:
- a) where possible, the identity, nationality and location of the person or persons who are the subject of the investigation, prosecution or proceeding in the Requesting State;
- b) available information on the identity and whereabouts of a person to be located in the Requested State;
- c) the identity and location of a person to be served, that person's relationship to the investigation, prosecution or proceeding, and the manner in which service is to be effected;
- d) the identity and location of persons from whom evidence is sought;

DOMESTIC LEGISLATION

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.

- e) in the case of requests for the taking of evidence or search and seizure, a statement indicating the basis for belief that evidence may be found in the jurisdiction of the Requested State;
- f) a precise description of the place to be searched and of the evidence to be searched for;
- g) the need, if any, for confidentiality and the reasons therefore;
- h) a description of the manner in which any testimony or statement is to be taken and recorded;
- i) a list of questions to be answered;
- j) in the case of requests to take evidence from a person, a statement as to whether sworn or affirmed statements are required, and a description of the subject matter of the evidence or statement sought;
- k) a description of any particular procedure to be followed in executing the request;
- I) information as to the allowances and expenses to which a person appearing in the Requesting State will be entitled;
- m) in the case of making detained persons available, the person or the authority who will have custody during the transfer, the place to which the detained person is to be transferred and the date of that person's return; and
- n) any other information which may be brought to the attention of the Requested State to facilitate its execution of the request.
- 4. If the Requested State considers that the information contained in the request is not sufficient to enable the request to be dealt with, that Party may request that additional details be furnished.

Article 6: Execution of requests

- 1. Requests for assistance shall be executed promptly in accordance with the law of the Requested State and, insofar as it is not prohibited by that law, in the manner requested by the Requesting State.
- 2. The Requested State shall not decline execution of a request on the ground of bank secrecy.

<u>Treaty between Thailand and Korea on Mutual Assistance in Criminal</u>
<u>Matters</u> (2003)

Article 5: Form and contents of requests

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
	1. A request shall be made in writing except that the Requested Party may accept a request in another form in urgent situations. In any such situation, the request shall be confirmed in writing promptly thereafter unless the Requested Party agrees otherwise.
	2. Requests for assistance shall include: (a) the name of the competent authority conducting the investigation, prosecution or proceeding to which the request relates; (b) the purpose of the request and the description of the assistance sought; and (c) the description of the subject matter and the nature of the investigation, prosecution or proceeding, including a summary of relevant facts and laws except in cases of request for service of documents.
	3. Requests for assistance, to the extent necessary and possible, shall also include:
	(a) information on the identity, nationality and location of the person or persons who are the subject of the investigation, prosecution or proceeding in the Requesting Party and of any person from whom evidence is sought;
	(b) information on the identity and location of a person to be served, that person's relationship to the proceeding, and the manner in which service is to be made;
	(c) information on the identity and whereabouts of a person or objects to be located;
	(d) a description of the person or place to be searched and of the objects to be seized;
	(e) a description of any particular procedure or requirement to be followed in executing the request;
	(f) information as to the allowances and expenses to which a person asked to appear in the Requesting Party will be entitled;
	(g) the need for confidentiality and the reasons therefore; (h) any time limit within which compliance with the request is desired;
	(i) a list of questions to be answered; and (j) such other information as is necessary for the proper execution of the request.
	4. If the Requested Party considers that the information contained in the request is not sufficient to enable the request to be dealt with, it may request

BUDAPEST CONVENTION DOMESTIC LEGISLATION additional information. 5. Requests, supporting documents and other communications made pursuant to this Treaty shall be accompanied by a translation into the language of the Requested Party or into the English language. Article 30 - Expedited disclosure of preserved traffic data CCA (2007, amended 2017) Chapter II: Competent officials 1 Where, in the course of the execution of a request made pursuant to Section 26 Article 29 to preserve traffic data concerning a specific communication, the A service provider is obliged to retain computer traffic data for at least ninety requested Party discovers that a service provider in another State was days from the date on which the data is entered into a computer system. If involved in the transmission of the communication, the requested Party shall necessary, on a particular provider and on a particular occasion, a competent expeditiously disclose to the requesting Party a sufficient amount of traffic official may instruct a service provider to retain such computer traffic data for data to identify that service provider and the path through which the longer than ninety days but not exceeding two years. communication was transmitted. Disclosure of traffic data under paragraph 1 may only be withheld if: Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992) the request concerns an offence which the requested Party considers a **Chapter 1: Central Authority** political offence or an offence connected with a political offence; or Section 7 the requested Party considers that execution of the request is likely to The Central Authority shall have the following authority and functions: prejudice its sovereignty, security, ordre public or other essential interests. (1) To receiving the request for assistance from the Requesting State and transmit it to the Competent Authorities; (2) To receive the request seeking assistance presented by the agency of the Royal Thai Government and deliver to the Requested State; (3) To consider and determine whether to provide or seek assistance; (4) To follow and expedite the performance of the Competent Authorities in providing assistance to a foreign state for the purpose of expeditious conclusion; (5) To issue regulations or announcement for the implementation of this Act; (6) To carry out other acts necessary for the success of providing or seeking assistance under this Act. Chapter 2: Providing of and seeking for assistance, Part 1: General provisions Section 9 The providing of assistance to a foreign state shall be subject to the following conditions: (1) Assistance may be provided even there exists no mutual assistance treaty

between Thailand and the Requesting State provides that such state commits to

assist Thailand under the similar manner when requested;

BUDAPEST CONVENTION DOMESTIC LEGISLATION (2) The act which is the cause of a request must be an offence punishable under Thai laws unless when Thailand and the Requesting State have a mutual assistance treaty between them and the treaty otherwise specifies provides, however, that the assistance must be conformed to the provisions of this Act; (3) A request may be refused if it shall affect national sovereignty or security, or other crucial public interests of Thailand, or relate to a political offence; (4) The providing of assistance shall not be related to a military offence. Section 11 Upon receipt a request for assistance from a foreign state, the Central Authority shall consider and determine whether such request is eligible for the providing of assistance under this Act and has followed the process correctly as well as accompanied by all appropriate supporting documents. If such request eligible for the providing of assistance, and in line with the process, as well as accompanied by all appropriate supporting documents, the Central Authority shall transmit the said request to the Competent Authorities for further execution. If such request if not eligible for the providing of assistance, or must be subject to some essential conditions before the assistance is provided, or if it is not in line with the process or has not been accompanied by all appropriate supporting documents required, the Central Authority shall refuse to provide assistance and notify the Requesting State the reasons thereof, or indicate the required conditions, or the causes of impossibility to execute the request. If the Central Authority is of the view that the execution of a request may interfere with the investigation, inquiry, prosecution, or other criminal proceeding pending its handling in Thailand, he may postpone the execution of the said request or may execute it under certain conditions set by him and notify the Requesting State about that. A determination of the Central Authority with regard to the providing of assistance shall be final, unless otherwise alliterated by the Prime Minister. Criteria for computer traffic data storage of service providers (2007) Article 31 - Mutual assistance regarding accessing of stored **CCA** (2007, amended 2017) **Chapter II: Competent officials** computer data Section 18

- 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:
- there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
- the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

With the enforcement of Section 19 and for the benefit of an investigation, when it could be reasonably believed that there is a perpetration of an offense under this Act, or there is a request per Paragraph Two, the competent official shall have one of the following powers necessary for the acquisition of evidence to prove the perpetration and to identify the perpetrators:

DOMESTIC LEGISLATION

- (1) issue an inquiry letter or summon any person related to the perpetration of an offense to testify, to explain in letter, or to submit any other document, data, or evidence in the comprehensible form;
- (2) request computer traffic data, from a service provider related to communication via computer system, or from other related persons;
- (3) instruct a service provider to surrender user-related data that must be retained under Section 26, or that is in the service provider's possession or control, to a competent official, or to keep the data for later;
- (4) make a copy of computer data and computer traffic data from a computer system reasonably believed to have been used for the perpetration of an offense, if that computer system is not yet in the possession of the competent official:
- (5) instruct a person, who is in possession or in control of computer data or a computer data storage device, to surrender the computer data or the device to the competent official:
- (6) inspect or access any person's computer system, computer data, computer traffic data, or computer data storage device, which is or can be used as evidence related to the perpetration of the offense; or which is for the identification of the perpetrator of the offense; and may instruct that person to surrender relevant computer data and computer traffic data to all necessary extent as well:
- (7) decrypt any person's computer data; or instruct any person related to the encryption of the computer data to decrypt the data, or to cooperate with a competent official in such decryption:
- (8) seize or forfeit a computer system as necessary for the benefit of obtaining details of the offense and the perpetrators of the offense.

For the benefit of the investigation and interrogation of the inquiry official per the Criminal Procedure Code, if there is a criminal offense against other laws which has made use of a computer system, computer data, or a computer storage device, as an accessory for the perpetration, or if there is computer data related to the perpetration of criminal offense against other laws, the inquiry

BUDAPEST CONVENTION DOMESTIC LEGISLATION official may request the competent official per Paragraph One to execute power per Paragraph One. Or if it dawns on the competent official as a result of the execution of duties per this Act, the competent official shall urgently compile facts and evidence and inform the relevant official for further action. The person receiving the request from the competent official as to Paragraph One (1), (2), and (3) shall without delay act as requested, but not longer than seven days since the day the request was received; or act within the time specified by the competent official, which shall not less than seven days and not exceeding fifteen days. Except when there is a reasonable cause and with permission from the competent official. The Minister may publish in the Government Gazette prescribing the duration to carry out the request as appropriate to types of the service provider. CCA (2007, amended 2017) Chapter II: Competent officials Section 26 A service provider is obliged to retain computer traffic data for at least ninety days from the date on which the data is entered into a computer system. If necessary, on a particular provider and on a particular occasion, a competent official may instruct a service provider to retain such computer traffic data for longer than ninety days but not exceeding two years.

Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992)

Chapter 1: Central Authority

Section 7

The Central Authority shall have the following authority and functions:

- (1) To receiving the request for assistance from the Requesting State and transmit it to the Competent Authorities;
- (2) To receive the request seeking assistance presented by the agency of the Royal Thai Government and deliver to the Requested State;
- (3) To consider and determine whether to provide or seek assistance;
- (4) To follow and expedite the performance of the Competent Authorities in providing assistance to a foreign state for the purpose of expeditious conclusion;
- (5) To issue regulations or announcement for the implementation of this Act;
- (6) To carry out other acts necessary for the success of providing or seeking assistance under this Act.

BUDAPEST CONVENTION DOMESTIC LEGISLATION Chapter 2: Providing of and seeking for assistance, Part 2: Inquiry and producing evidence Section 15 Upon receipt the request for assistance from a foreign state to take statement of persons or gathering evidence located in Thailand at the stage of inquiry, the Competent Authorities shall direct an inquiry official to execute such request. The Inquiry Official shall have authority to take statement of persons or gathering evidence as requested under paragraph one and, if necessary, to search and seize any document or article in accordance with rules, means, and contentions set forth in the Criminal Procedure Code. When the taking statement of persons or gathering evidence has been finished, the Inquiry Official shall report and deliver all evidence derived from to the Competent Authorities. Chapter 2: Providing of and seeking for assistance, Part 5: Search and seizure Section 23 Upon receipt the request for assistance from a foreign state to search or seize and deliver any article, the Competent Authorities shall have the power to search or issue a warrant of search and seize in accordance with the law, if there shall be a reasonable ground to do so. Section 24 As regards the search and seizure under Section 23, the provisions relating to search under the Criminal Procedure Code shall be applied, mutatis mutandis. Section 25 The Competent Authorities conducting search or seizure of article in compliance with the request for assistance shall certify the continuity of custody, identity of the article, as well as integrity of its condition, and shall deliver the said article together with the certificate thereof to the Central Authority.

the Central Authority.

The certificate thereof shall be in the form and in line with the means defined by

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
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	Chapter 2: Providing of and seeking for assistance, Part 9: Forfeiture or seizure of properties Section 32 Upon receipt the request for assistance from a foreign state to forfeit or seize properties located in Thailand, the Competent Authorities shall apply to the Court having jurisdiction over the location of the properties for passing the judgment forfeiting such properties or for the issuance of an order seizing them. Under paragraph one, the Competent authorities shall, if it is necessary, conduct an inquiry himself or authorizes any inquiry official to conduct an inquiry on his behalf. Section 34 The provision related to forfeiture of properties set forth in the Criminal Procedure Code and the Penal Code shall be applied to the inquiry, the application of motion, the trail, the adjudication, and the issuance of an order to forfeit or seize of properties in this regard, mutatis mutandis. Section 35 The properties forfeited by the judgment of the Court under this part shall become the properties of the State, but the Court may pass judgment for such properties to be rendered useless, or to be destroyed. N/A
data to the Party through that computer system.	
Article 33 - Mutual assistance in the real-time collection of traffic data	CCA (2007, amended 2017) Chapter II: Competent officials Section 18
1 The Parties shall provide mutual assistance to each other in the real-time	J ,
collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the	

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.

have one of the following powers necessary for the acquisition of evidence to prove the perpetration and to identify the perpetrators:

- (1) issue an inquiry letter or summon any person related to the perpetration of an offense to testify, to explain in letter, or to submit any other document, data, or evidence in the comprehensible form;
- (2) request computer traffic data, from a service provider related to communication via computer system, or from other related persons;
- (3) instruct a service provider to surrender user-related data that must be retained under Section 26, or that is in the service provider's possession or control, to a competent official, or to keep the data for later;
- (4) make a copy of computer data and computer traffic data from a computer system reasonably believed to have been used for the perpetration of an offense, if that computer system is not yet in the possession of the competent official;
- (5) instruct a person, who is in possession or in control of computer data or a computer data storage device, to surrender the computer data or the device to the competent official;
- (6) inspect or access any person's computer system, computer data, computer traffic data, or computer data storage device, which is or can be used as evidence related to the perpetration of the offense; or which is for the identification of the perpetrator of the offense; and may instruct that person to surrender relevant computer data and computer traffic data to all necessary extent as well;
- (7) decrypt any person's computer data; or instruct any person related to the encryption of the computer data to decrypt the data, or to cooperate with a competent official in such decryption;
- (8) seize or forfeit a computer system as necessary for the benefit of obtaining details of the offense and the perpetrators of the offense.

For the benefit of the investigation and interrogation of the inquiry official per the Criminal Procedure Code, if there is a criminal offense against other laws which has made use of a computer system, computer data, or a computer storage device, as an accessory for the perpetration, or if there is computer data related to the perpetration of criminal offense against other laws, the inquiry official may request the competent official per Paragraph One to execute power per Paragraph One. Or if it dawns on the competent official as a result of the execution of duties per this Act, the competent official shall urgently compile

BUDAPEST CONVENTION DOMESTIC LEGISLATION facts and evidence and inform the relevant official for further action. The person receiving the request from the competent official as to Paragraph One (1), (2), and (3) shall without delay act as requested, but not longer than seven days since the day the request was received; or act within the time specified by the competent official, which shall not less than seven days and not exceeding fifteen days. Except when there is a reasonable cause and with permission from the competent official. The Minister may publish in the Government Gazette prescribing the duration to carry out the request as appropriate to types of the service provider. CCA (2007, amended 2017) Chapter II: Competent officials Section 26 A service provider is obliged to retain computer traffic data for at least ninety days from the date on which the data is entered into a computer system. If necessary, on a particular provider and on a particular occasion, a competent official may instruct a service provider to retain such computer traffic data for longer than ninety days but not exceeding two years. Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992) Chapter 1: Central Authority Section 7 The Central Authority shall have the following authority and functions: (1) To receiving the request for assistance from the Requesting State and transmit it to the Competent Authorities; (2) To receive the request seeking assistance presented by the agency of the Royal Thai Government and deliver to the Requested State; (3) To consider and determine whether to provide or seek assistance; (4) To follow and expedite the performance of the Competent Authorities in providing assistance to a foreign state for the purpose of expeditious conclusion; (5) To issue regulations or announcement for the implementation of this Act; (6) To carry out other acts necessary for the success of providing or seeking assistance under this Act. Chapter 2: Providing of and seeking for assistance, Part 2: Inquiry and

producing evidence

Section 15

BUDAPEST CONVENTION DOMESTIC LEGISLATION Upon receipt the request for assistance from a foreign state to take statement of persons or gathering evidence located in Thailand at the stage of inquiry, the Competent Authorities shall direct an inquiry official to execute such request. The Inquiry Official shall have authority to take statement of persons or gathering evidence as requested under paragraph one and, if necessary, to search and seize any document or article in accordance with rules, means, and contentions set forth in the Criminal Procedure Code. When the taking statement of persons or gathering evidence has been finished, the Inquiry Official shall report and deliver all evidence derived from to the Competent Authorities. Chapter 2: Providing of and seeking for assistance, Part 5: Search and seizure Section 23 Upon receipt the request for assistance from a foreign state to search or seize and deliver any article, the Competent Authorities shall have the power to search or issue a warrant of search and seize in accordance with the law, if there shall be a reasonable ground to do so. Section 24 As regards the search and seizure under Section 23, the provisions relating to search under the Criminal Procedure Code shall be applied, mutatis mutandis. Section 25 The Competent Authorities conducting search or seizure of article in compliance with the request for assistance shall certify the continuity of custody, identity of the article, as well as integrity of its condition, and shall deliver the said article together with the certificate thereof to the Central Authority. The certificate thereof shall be in the form and in line with the means defined by the Central Authority. Chapter 2: Providing of and seeking for assistance, Part 9: Forfeiture or seizure of properties

Section 32

BUDAPEST CONVENTION DOMESTIC LEGISLATION Upon receipt the request for assistance from a foreign state to forfeit or seize properties located in Thailand, the Competent Authorities shall apply to the Court having jurisdiction over the location of the properties for passing the judgment forfeiting such properties or for the issuance of an order seizing them. Under paragraph one, the Competent authorities shall, if it is necessary, conduct an inquiry himself or authorizes any inquiry official to conduct an inquiry on his behalf. Section 34 The provision related to forfeiture of properties set forth in the Criminal Procedure Code and the Penal Code shall be applied to the inquiry, the application of motion, the trail, the adjudication, and the issuance of an order to forfeit or seize of properties in this regard, mutatis mutandis. Section 35 The properties forfeited by the judgment of the Court under this part shall become the properties of the State, but the Court may pass judgment for such properties to be rendered useless, or to be destroyed.

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.

CCA (2007, amended 2017) Chapter II: Competent officials Section 18

With the enforcement of Section 19 and for the benefit of an investigation, when it could be reasonably believed that there is a perpetration of an offense under this Act, or there is a request per Paragraph Two, the competent official shall have one of the following powers necessary for the acquisition of evidence to prove the perpetration and to identify the perpetrators:

Criteria for computer traffic data storage of service providers (2007)

- (1) issue an inquiry letter or summon any person related to the perpetration of an offense to testify, to explain in letter, or to submit any other document, data, or evidence in the comprehensible form;
- (2) request computer traffic data, from a service provider related to communication via computer system, or from other related persons;
- (3) instruct a service provider to surrender user-related data that must be retained under Section 26, or that is in the service provider's possession or control, to a competent official, or to keep the data for later;
- (4) make a copy of computer data and computer traffic data from a computer

BUDAPEST CONVENTION DOMESTIC LEGISLATION system reasonably believed to have been used for the perpetration of an offense, if that computer system is not yet in the possession of the competent official: (5) instruct a person, who is in possession or in control of computer data or a computer data storage device, to surrender the computer data or the device to the competent official; (6) inspect or access any person's computer system, computer data, computer traffic data, or computer data storage device, which is or can be used as evidence related to the perpetration of the offense; or which is for the identification of the perpetrator of the offense; and may instruct that person to surrender relevant computer data and computer traffic data to all necessary extent as well; (7) decrypt any person's computer data; or instruct any person related to the encryption of the computer data to decrypt the data, or to cooperate with a competent official in such decryption; (8) seize or forfeit a computer system as necessary for the benefit of obtaining details of the offense and the perpetrators of the offense. For the benefit of the investigation and interrogation of the inquiry official per the Criminal Procedure Code, if there is a criminal offense against other laws which has made use of a computer system, computer data, or a computer storage device, as an accessory for the perpetration, or if there is computer data related to the perpetration of criminal offense against other laws, the inquiry official may request the competent official per Paragraph One to execute power per Paragraph One. Or if it dawns on the competent official as a result of the execution of duties per this Act, the competent official shall urgently compile facts and evidence and inform the relevant official for further action. The person receiving the request from the competent official as to Paragraph One (1), (2), and (3) shall without delay act as requested, but not longer than seven days since the day the request was received; or act within the time specified by the competent official, which shall not less than seven days and not exceeding fifteen days. Except when there is a reasonable cause and with permission from the competent official. The Minister may publish in the

Government Gazette prescribing the duration to carry out the request as

appropriate to types of the service provider.

BUDAPEST CONVENTION DOMESTIC LEGISLATION Act on Mutual Assistance in Criminal Matters B.E. 2535 (1992) Chapter 1: Central Authority Section 7 The Central Authority shall have the following authority and functions: (1) To receiving the request for assistance from the Requesting State and transmit it to the Competent Authorities; (2) To receive the request seeking assistance presented by the agency of the Royal Thai Government and deliver to the Requested State; (3) To consider and determine whether to provide or seek assistance; (4) To follow and expedite the performance of the Competent Authorities in providing assistance to a foreign state for the purpose of expeditious conclusion; (5) To issue regulations or announcement for the implementation of this Act; (6) To carry out other acts necessary for the success of providing or seeking assistance under this Act. Chapter 2: Providing of and seeking for assistance, Part 2: Inquiry and producing evidence Section 15 Upon receipt the request for assistance from a foreign state to take statement of persons or gathering evidence located in Thailand at the stage of inquiry, the Competent Authorities shall direct an inquiry official to execute such request. The Inquiry Official shall have authority to take statement of persons or gathering evidence as requested under paragraph one and, if necessary, to search and seize any document or article in accordance with rules, means, and contentions set forth in the Criminal Procedure Code. When the taking statement of persons or gathering evidence has been finished, the Inquiry Official shall report and deliver all evidence derived from to the Competent Authorities. Chapter 2: Providing of and seeking for assistance, Part 5: Search and seizure Section 23 Upon receipt the request for assistance from a foreign state to search or seize

and deliver any article, the Competent Authorities shall have the power to search or issue a warrant of search and seize in accordance with the law, if

BUDAPEST CONVENTION DOMESTIC LEGISLATION there shall be a reasonable ground to do so. Section 24 As regards the search and seizure under Section 23, the provisions relating to search under the Criminal Procedure Code shall be applied, mutatis mutandis. Section 25 The Competent Authorities conducting search or seizure of article in compliance with the request for assistance shall certify the continuity of custody, identity of the article, as well as integrity of its condition, and shall deliver the said article together with the certificate thereof to the Central Authority. The certificate thereof shall be in the form and in line with the means defined by the Central Authority. Chapter 2: Providing of and seeking for assistance, Part 9: Forfeiture or seizure of properties Section 32 Upon receipt the request for assistance from a foreign state to forfeit or seize properties located in Thailand, the Competent Authorities shall apply to the Court having jurisdiction over the location of the properties for passing the judgment forfeiting such properties or for the issuance of an order seizing them. Under paragraph one, the Competent authorities shall, if it is necessary, conduct an inquiry himself or authorizes any inquiry official to conduct an inquiry on his behalf. Section 34 The provision related to forfeiture of properties set forth in the Criminal Procedure Code and the Penal Code shall be applied to the inquiry, the application of motion, the trail, the adjudication, and the issuance of an order to forfeit or seize of properties in this regard, mutatis mutandis. Section 35 The properties forfeited by the judgment of the Court under this part shall become the properties of the State, but the Court may pass judgment for such

properties to be rendered useless, or to be destroyed.

BUDAPEST CONVENTION	DOMESTIC LEGISLATION
Article 35 – 24/7 Network 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a the provision of technical advice; b the preservation of data pursuant to Articles 29 and 30; c the collection of evidence, the provision of legal information, and locating of suspects. 2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.	N/A
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.	