

KINGDOM OF CAMBODIA

LAW ON ELECTRONIC COMMERCE

Part 1 General Provisions

- Article 1: Purpose
- Article 2: Sphere of Application
- Article 3: Variation by Agreement
- Article 4: Definitions

PART 2 – VALIDITY OF DATA MESSAGES AND ELECTRONIC COMMUNICATIONS

- Article 5: Legal recognition of data messages and electronic communications
- Article 6: Writing requirements
- Article 7: Signature requirements
- Article 8: Original Requirements
- Article 9: Record Retention Requirements
- Article 10: Evidential requirements
- Article 11: Contract formation
- Article 12: Declarations and other statements

PART 3 – COMMUNICATIONS PROCESS

- Article 13: Attribution
- Article 14: Time and place of dispatch and receipt of data messages

PART 4 – CERTIFICATION SERVICE PROVIDERS

- Article 15: Issuance of Regulations

PART 5 – GOVERNMENT ACTS AND TRANSACTIONS

- Article 16: Acceptance of data messages

PART 6 – OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF INFORMATION SYSTEMS AND COMPUTER DATA

- Article 17: Illegal access
- Article 18: Illegal interception
- Article 19: Data interference
- Article 20: System interference
- Article 21: Computer data-related forgery
- Article 22: Computer-related fraud
- Article 23: Incitement, aiding or abetting, complicity or attempt
- Article 24: Penalties

PART 1 – GENERAL PROVISIONS

Article 1: Purpose

This law is designed to achieve the following objectives and should be construed accordingly:

- (a) to facilitate domestic and international electronic commerce by eliminating legal barriers and establishing legal certainty;
- (b) to encourage the use of reliable forms of electronic commerce;
- (c) to facilitate electronic filing of documents with Government and to promote efficient delivery of Government services by means of reliable forms of electronic communications;
- (d) to promote public confidence in the authenticity, integrity and reliability of data messages and electronic communications;
- (e) to deter the commission of harmful conduct against computer data and information systems.

Article 2: Sphere of Application

- (1) Parts 2 through 5 of this Law shall apply to all civil and commercial acts and transactions, except those acts and transactions exempted under the terms of this Act or by Government legislation.
- (2) Nothing in Parts 2 through 5 of this Law affects the application of any rule of law that may require the parties to disclose their identities, places of business or other information, or relieves a party from the legal consequences of making inaccurate or false statements in that regard.
- (3) Parts 2 through 4 of this Law shall apply to acts and transactions carried out by or with the Government in accordance with Part 5.

Article 3: Variation by Agreement

The provisions of Part 2 and Part 3 may be varied by agreement between parties involved in generating, sending, receiving, storing, or otherwise processing data messages, except as otherwise provided.

Article 4: Definitions

The definition of terms used in this Law shall be as follows:

‘Addressee’ of an electronic communication means a party who is intended by the originator to receive the electronic communication, but does not include a party acting as an intermediary with respect to that electronic communication;

“Automated message system” means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a person each time an action is initiated or a response is generated by the system;

‘Certification Service Provider’ means a person that issues certificates and may provide other services related to electronic signatures;

‘Computer data’ means any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function;

‘Data message’ means information generated, sent, received or stored by electronic, magnetic, optical or similar means;

‘Electronic communication’ means any communication that the parties make by means of data messages;

‘Electronic signature’ means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory’s approval of the information contained in the data message;

‘Information system’ means any device or a group of interconnected or related devices for generating, sending, receiving, storing or otherwise processing Computer data, including Data messages;

‘Originator’ of an electronic communication means a party by whom, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but it does not include a party acting as an intermediary with respect to that electronic communication;

PART 2 – VALIDITY OF DATA MESSAGES AND ELECTRONIC COMMUNICATIONS

Article 5: Legal recognition of data messages and electronic communications

- (1) Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.
- (2) A communication or a contract shall not be denied validity or enforceability on the sole ground that it is in the form of an electronic communication.

Article 6: *Writing requirements*

- (1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.
- (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.
- (3) The provisions of this article do not apply to the following requirements for information to be in writing:

[...]

Comment [INZ1]: E.g. sale of land.
To be discussed by the Drafting Committee

Article 7: *Signature requirements*

- (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
- (2) Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.
- (3) An electronic signature is presumed to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
 - (a) it is uniquely linked to the signatory;
 - (b) it is capable of identifying the signatory;
 - (c) it is created using means that the signatory can maintain under his sole control; and
 - (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.
- (4) Paragraph 3 does not limit the ability of any person:
 - (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or
 - (b) To adduce evidence of the non-reliability of an electronic signature.

- (5) The provisions of this article do not apply to the following requirements for a signature:

[...]

Comment [INZ2]: e.g. a will

Article 8: *Original Requirements*

- (1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:
- (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
 - (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.
- (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.
- (3) For the purposes of subparagraph (a) of paragraph (1):
- (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
 - (b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

Article 9: *Record Retention Requirements*

- (1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:
- (a) the information contained therein is accessible so as to be usable for subsequent reference; and
 - (b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

- (c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.
- (2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

Article 10: *Evidential requirements*

- (1) In any legal proceedings, nothing in the application of the rules of evidence under [.....] shall apply so as to deny the admissibility of a data message in evidence:
 - (a) on the sole ground that it is a data message; or,
 - (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.
- (2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, a court shall have regard to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

Comment [INZ3]: This should reference the relevant civil procedure rules and, or, or commercial court rules.

Article 11: *Contract formation*

- (1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.
- (2) A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.
- (3) A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability on the sole ground that no natural person reviewed each of the individual actions carried out by the systems or the resulting contract.

- (4) Nothing in this Law affects the application of any rule of law that may require a party that negotiates some or all of the terms of a contract through the exchange of electronic communications to make available to the other party those electronic communications that contain the contractual terms in a particular manner, or relieves a party from the legal consequences of its failure to do so.
- (5) The provisions of this article do not apply to the following types of contract:

[...]

Comment [INZ4]: This reflects Article 2 of the UNCITRAL 2005 Convention.

Article 12: *Declarations and other statements*

As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

PART 3 – COMMUNICATIONS PROCESS

Article 13: *Attribution*

- (1) A data message is that of the originator if it was sent by the originator itself.
- (2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:
 - (a) by a person who had the authority to act on behalf of the originator in respect of that data message; or
 - (b) by an information system programmed by, or on behalf of, the originator to operate automatically.
- (3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:
 - (a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
 - (b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

- (4) Paragraph (3) does not apply:
- (a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or
 - (b) in a case within paragraph (3)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.
- (5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.
- (6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14: *Time and place of dispatch and receipt of data messages*

- (1) The time of dispatch of an electronic communication is the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator or, if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.
- (2) The time of receipt of an electronic communication is the time when it becomes capable of being retrieved by the addressee at an electronic address designated by the addressee. The time of receipt of an electronic communication at another electronic address of the addressee is the time when it becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address. An electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.
- (3) An electronic communication is deemed to be dispatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business.

- (4) Paragraph 2 of this article applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under paragraph 3 of this article.

PART 4 – CERTIFICATION SERVICE PROVIDERS

Article 15: Issuance of Regulations

- (1) With the approval of the Prime Minister, and in consultation with other Ministerial Departments, the Ministry of Commerce is empowered, where it considers necessary, to draft and issue regulations governing all or any the following matters:

Comment [INZ5]: Or which ever Ministry or department is considered most appropriate.

- (a) The right of Certification Service Providers to establish and provide certification services in the Kingdom of Cambodia;
 - (b) the terms and conditions under which Certification Service Providers may offer certification services to persons;
 - (c) the standards with which Certification Service Providers are required to comply;
 - (d) the legal recognition of foreign Certification Service Providers, any certificates issued by them or the provision of other services .
- (2) In the course of drafting regulations under this article, [.....] has a duty to give full and due consideration to recommendations, policies and standards endorsed by the ASEAN Secretariat or other relevant organisations.

PART 5 – GOVERNMENT ACTS AND TRANSACTIONS

Article 16: Acceptance of data messages

- (1) Any part of the Government that, pursuant to any law:
- (a) accepts the filing of documents, or requires that documents be created or retained;
 - (b) issues any permit, licence or approval; or
 - (c) provides for the method and manner of payment,
- may, notwithstanding anything to the contrary in such written law —
- (i) accept the filing of such documents, or the creation or retention of such documents in the form of data messages;
 - (ii) issue such permit, licence or approval in the form of data messages; or
 - (iii) make such payment in electronic form.

- (2) In any case where a part of the Government decides to perform any of the functions in subsection (1) (i), (ii) or (iii), such agency may specify:
- (a) The manner and format in which such data message or electronic communication shall be filed, created, retained or issued;
 - (b) Where such data messages have to be signed, the type of electronic signature required;
 - (c) The manner and format in which such signature shall be affixed to the data message;
 - (d) Control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of data messages, electronic communication or payments; and
 - (e) Any other required attributes for data messages, electronic communication or payments that are currently specified for corresponding paper documents.
- (3) Nothing in this Act shall by itself compel any part of the Government to accept or issue any document in the form of data messages.

PART 6 – OFFENCES AGAINST THE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY OF INFORMATION SYSTEMS AND COMPUTER DATA

Comment [INZ6]: Should this comprise an amendment to the Criminal Code or be stand-alone?

Article 17: Illegal access

It shall be an offence for any person to commit intentionally, the access to the whole or any part of an information system knowing or having reason to believe that he is not authorised to secure such access.

Article 18: Illegal interception

It shall be an offence, when committed intentionally, for any person to unlawfully intercept, by technical means, any non-public transmission of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data.

Article 19: Data interference

It shall be an offence for any person, intentionally and without right, to damage, delete, deteriorate, alter, suppress or render inaccessible computer data on an information system.

Article 20: System interference

It shall be an offence for any person, intentionally and without right, to interfere with the functioning of an information system by inputting, transmitting,

damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data.

Article 21: *Computer data-related forgery*

It shall be an offence, when committed intentionally and without right, for any person to input, alter, delete or suppress 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.

Article 22: *Computer-related fraud*

It shall be an offence, when committed intentionally and without right, for any person to cause a loss of property to another person by:

- (1) any input, alteration, deletion or suppression of computer data;
- (2) any interference with the functioning of an information system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 23: *Incitement, aiding or abetting, complicity or attempt*

- (1) It shall be an offence, when committed intentionally, to incite, aid or abet others, or are complicit with others, in the commission of any of the offences referred to in articles 17 through 22 of this Law.
- (2) It shall be an offence, when committed intentionally, to attempt to commit any of the offences referred to in articles 17 through 22 of this Law.

Article 24: *Penalties*

A person found guilty of committing one or more of the offences under Part 6 of this Law may be liable on conviction to a term of imprisonment and, or, fine in accordance with the following **schedule**:

Comment [INZ7]: The level of penalties will need to be determined by reference to the Criminal Code.