Electronic Transactions Act [Cap 263]

LAWS OF THE REPUBLIC OF VANUATU
CONSOLIDATED EDITION 2006

Commencement: 6 November 2000

CHAPTER 263
ELECTRONIC TRANSACTIONS

Act 24 of 2000

ARRANGEMENT OF SECTIONS

ELECTRONIC TRANSACTIONS

An Act to make provision for electronic transactions, and for related matters.

PART 1 – PRELIMINARY

1. Definitions

In this Act, unless the contrary intention appears:

"accredited certificate" means an electronic record that:

(a) associates a signature verification device to a person; and

(b) confirms the identity of that person; and

(c) is issued by an authorised certification service provider under section 20;

"addressee", in relation to an electronic record, means a person who is intended by the originator to receive the electronic record, but does not include a person acting as an intermediary with respect to that electronic record;

"appropriate law enforcement agency" means:

(a) the Public Prosecutor; or

(b) the Attorney General; or

(c) a person prescribed for the purposes of any provision of this Act in which the expression occurs;

"approved form" means a form approved by the Minister for use under this Act;

"authorised certification service provider" means a certification service provider authorised under section 20(2) to provide accredited certificates;

"certification service provider" means a person who issues identity certificates for the purposes of electronic signatures or provides other services to the public related to electronic signatures;

"data controller" means a person who, either alone or jointly or in common with other persons, determines the purposes for which and the manner in which any personal data is, or is to be, processed;

"data processor" means a person who processes personal data on behalf of a data controller;

"e-commerce service provider" means a person who uses electronic means in providing goods, services or information;

"electronic agent device" means a program, or other electronic or automated means, that is used to initiate or respond to electronic records;

"electronic record" means a record created, stored, generated, received or communicated by electronic means;

"electronic signature" means a signature in electronic form in, attached to, or logically associated with, information that is used by a signatory to indicate his or her adoption of the content of that information and meets the following requirements:

(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 or her sole control;

(d) it is linked to the information to which it relates in such a manner that any subsequent alteration of the information is revealed;

"electronic signature product" means hardware or software, or components of either, that are intended to be used by a certification service provider for the provision of electronic signature services;

"identifiable individual" means an individual who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physiological, mental, economic, cultural or social identity;

"information" includes data, text, images, sounds, codes, computer programs, software and databases;

"information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying or otherwise processing information;

"intermediary", in relation to an electronic record, means a person who, on behalf of another person, sends, receives or stores that electronic record or provides other services with respect to that electronic record;

"Minister" means the Minister responsible for telecommunications and electronic commerce;

"originator", in relation to an electronic record, means a person by whom, or on whose behalf, the electronic record purports to have been sent or generated prior to storage (if any) but does not include a person acting as an intermediary with respect to that electronic record;

"personal data" means any information relating to an identified or identifiable individual;

"prescribed" means prescribed by the regulations made under this Act;

"record" means information that is inscribed on a tangible medium or that is stored in an electronic, paper-based or any other medium and is retrievable in perceivable form;

"signature creation device" means unique data or a uniquely configured physical device which is used by the signatory in creating an electronic signature;

"signature verification device" means unique data or a uniquely configured physical device which is used in verifying an electronic signature.

2. Objects

The objects of this Act are:

(a) to enhance the reputation of Vanuatu as an international business centre; and

(b) to facilitate electronic transactions by means of reliable electronic records; and

(c) to remove uncertainties in relation to conducting transactions electronically with respect to the requirements for documents and for signatures to be in writing; and

(d) to promote public confidence in the validity, integrity and reliability of conducting transactions electronically; and

(e) to promote the development of the legal and business infrastructure necessary to implement electronic transactions securely.

3. Regulatory policy

The Government is to regulate transactions carried out by electronic means so as to:

(a) permit and encourage the growth of business by electronic means through the operation of free market forces; and

(b) promote the greatest possible use of industry self-regulation.

4. Government not obliged to use electronic records

Nothing in this Act obliges any ministry, department or agency of the government to

generate, send, receive, store or otherwise process any record by electronic means.

5. Acceptance of electronic records by the Government

The Minister may, by notice published in the Gazette, indicate that a ministry, department or agency of the government will receive and process electronic records relating to such matters as may be specified in the notice.

6. General exclusions

Parts 2 and 3 do not apply to any rule of law requiring writing or signatures for the following matters:

(a) the creation, execution or revocation of a will or testamentary instrument;

(b) the conveyance of real property or the transfer of any interest in real property.

7. Exclusions by Minister

The Minister may, by order in writing, provide that this Act, or such provisions as are specified in the order, do not apply to any class of transactions, persons, matters or things specified in the order.

PART 2 – LEGAL REQUIREMENTS FOR ELECTRONIC RECORDS

8. Legal recognition of electronic records

Information is not to be denied legal effect, validity, admissibility or enforceability solely on the ground that it is:

(a) in the form of an electronic record; or

(b) not contained in the electronic record purporting to give rise to such legal effect, but is referred to in that electronic record.

9. Writing

(1) If information is:

(a) required by law to be in writing; or
(b) described in any statutory provision as being written;
that requirement or description is met by an electronic record if the information contained in the electronic record is accessible and is capable of retention for subsequent reference.

(2) Subsection (1) applies whether the requirement for the information to be in writing is in the form of an obligation or the law provides consequences if it is not in writing.

10. Delivery

(1) If information is required by law to be delivered, dispatched, given or sent to, or to be served on a person, that requirement is met by doing so in the form of an electronic record if:

(a) the originator of the electronic record states that the receipt of the electronic record is to be acknowledged; and
(b) the addressee has acknowledged its receipt.

(2) Subsection (1) applies whether the requirement for delivery, dispatch, giving, sending or serving is in the form of an obligation or the law provides consequences for the information not being delivered, dispatched, given, sent or served.

11. Signature

(1) If the signature of a person is required by law, that requirement is met by an electronic record if:

(a) a method is used to identify that person and to indicate that he or she intended to sign or otherwise adopt the information in the electronic record; and

(b) that method is as reliable as is appropriate for the purpose for which the electronic

record was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) An electronic record that meets the requirements of subsections (1) (a) and (1) (b) is not to be denied legal effect, validity and enforceability solely on the ground that it:

(a) is not an electronic signature; or

(b) is not associated with an accredited certificate.

(3) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the law provides consequences for the absence of a signature.

12. Original form

(1) If information is required by law to be presented or retained in its original form, that requirement is met by an electronic record if:

(a) there exists a reliable assurance as to the integrity of the information from the time it was first generated in its final form as an electronic record or otherwise; and

(b) where it is required that information be presented, that information is capable of being accurately represented to the person to whom it is to be presented.

(2) Subsection (1) applies whether the requirement for the information to be presented or retained in its original form is in the form of an obligation or the law provides consequences if it is not presented or retained in its original form.

(3) For the purposes of subsection (1) (a):

(a) the criterion for assessing integrity is 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 is to be assessed in the light of the purpose for which the information was generated and all the relevant circumstances.

13. Retention of electronic records

(1) If certain documents, records or information are required by law to be retained, that requirement is met by retaining electronic records if the following conditions are satisfied:

(a) the information contained in the electronic record is accessible and is capable of retention for subsequent reference;

(b) the electronic record 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;

(c) any information that enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, is retained.

(2) An obligation to retain documents, records or information in accordance with subsection (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions set out in paragraphs (a), (b) and (c) of subsection (1) are met.

14. Admissibility and evidential weight of electronic records

(1) In any legal proceedings, nothing in the rules of evidence is to apply so as to deny the admissibility of an electronic record in evidence:

(a) solely on the ground that it is an electronic record; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the ground that it is not in its original form.

(2) Information in the form of an electronic record is to be given due evidential weight and in assessing the evidential weight of an electronic record, regard is to be had to:

(a) the reliability of the manner in which the electronic record was generated, stored or communicated; and

(b) the reliability of the manner in which the integrity of the information was maintained; and

(c) the manner in which the originator was identified; and

(d) any other relevant factor.

PART 3 – COMMUNICATION OF ELECTRONIC RECORDS

15. Formation and validity of contracts

(1) In the context of the formation of contracts, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic records.

(2) As between the originator and the addressee of an electronic record, a declaration of intention or other statement or delivery of a deed is not to be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

16. Attribution of electronic records

(1) An electronic record is attributable to a person if the electronic record resulted from the action of the person, by the person’s agent or the person’s electronic agent device.

(2) Attribution may be proven in any manner, including by showing the efficacy of any security procedure applied to determine the person to whom the electronic record was attributable.

17. Acknowledgement of receipt of electronic records

(1) Subsections (2), (3) and (4) apply where, on or before sending an electronic record, or by means of that electronic record, the originator has requested or has agreed with the addressee that receipt of the electronic record be acknowledged.

(2) If the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by:

(a) any communication by the addressee, automated or otherwise; or

(b) any conduct of the addressee; that is reasonably sufficient to indicate to the originator that the electronic record has been received.

(3) If the originator has stated that the electronic record is conditional on receipt of the acknowledgement, the electronic record is to be treated as though it had never been sent until the acknowledgement is received.

(4) If the originator has not stated that the electronic record is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in paragraph (a), may, upon notice to the addressee, treat the electronic record as though it had never been sent or exercise any other rights the originator may have.

(5) If the originator receives the addressee's acknowledgement of receipt, it is presumed that the related electronic record was received by the addressee, but that presumption does not imply that the electronic record corresponds to the record received.

(6) Except in so far as it relates to the sending or receipt of the electronic record, this section is not intended to deal with the legal consequences that may flow either from that electronic record or from the acknowledgement of its receipt.

18. Time and place of dispatch and receipt of electronic records

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of an electronic record occurs when it enters an information processing system outside the control of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic record is determined as follows:

(a) if the addressee has designated an information processing system for the purpose of receiving electronic records, receipt occurs:
(i) at the time when the electronic record enters the designated information processing system; or
(ii) if the electronic record is sent to an information processing system of the addressee that is not the designated information processing system, at the time when the electronic record comes to the attention of the addressee; or

(b) if the addressee has not designated an information processing system, receipt occurs when the electronic record enters an information processing system of the addressee or otherwise comes to the attention of the addressee.

(3) Subsection (2) applies notwithstanding that the place where the information processing system is located may be different from the place where the electronic record is taken to be received under subsection (4).

(4) Unless otherwise agreed between the originator and the addressee, an electronic record is taken to be dispatched at the place where the originator has his or her place of business, and is taken to be received at the addressee’s place of business.

(5) For the purposes of subsection (4):

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the transaction to which the electronic record relates or, where there is no such transaction, the place of business is presumed to be the principal place of business; or

(b) if the originator or the addressee does not have a place of business, it is presumed to be where the originator or the addressee ordinarily resides.

PART 4 – ELECTRONIC SIGNATURES

19. Electronic signature associated with an accredited certificate

An electronic signature that is associated with an accredited certificate issued by an authorised certification service provider under section 20 is taken to satisfy the requirements of section 11(1) (a) and (b).

20. Certification and revocation of certification

(1) A person may apply to the Minister for authorisation to provide accredited certificates.

(2) The application must be in the approved form and be accompanied by the prescribed fee.

(3) The Minister may, if satisfied that the applicant:
(a) has the knowledge and expertise to provide accredited certificates; and
(b) has the technical capabilities to provide accredited certificates; and
(c) meets any other prescribed criteria by notice published in the Gazette, authorise the applicant to provide accredited certificates.

(4) Subject to subsection (5), the Minister, if satisfied that an authorised certification service provider no longer meets the criteria in paragraphs (a), (b) and (c) of subsection (3), may by notice published in the Gazette revoke an authorisation.

(5) Before revoking an authorisation, the Minister must give the authorised certification service provider written notice:
(a) stating the Minister intends to revoke the authorisation; and
(b) indicating the reasons for the proposed revocation; and
(c) inviting that person, within 14 days of the notice, to submit representations in writing as to why the authorisation should not be revoked.

(6) The Minister must consider any such representations in deciding whether to revoke the authorisation and give the authorised certification service provider written notice of his or her decision within 7 days after making it.

(7) The revocation takes effect on the date specified in the notice.

21. Recognition of external certification service providers

(1) The Minister may, by notice published in the Gazette, recognise:
(a) certificates or classes of certificates issued in other jurisdictions; or
(b) certification service providers or classes of certification service providers established in other jurisdictions.

(2) Upon publication of the notice and on payment of the prescribed fee:

(a) those certificates or classes of certificates are taken to be accredited certificates; and

(b) those certification service providers or classes of certification service providers are taken to be authorised under section 20(2).

(3) In determining whether to accord recognition under subsection (1) the Minister must have regard to whether:

(a) the certificates or classes of certificates are required to, and do in fact, meet obligations equivalent to those required for an accredited certificate; and

(b) the certification service providers or classes of certification service providers are required to, and do in fact, meet criteria equivalent to those required for an authorised certification service provider.

(4) The Minister may, by notice published in the Gazette, revoke any recognition accorded under subsection (1).
(5) Before revoking any recognition, the Minister must give the person affected by the proposed revocation written notice:
(a) stating the Minister intends to revoke the recognition; and
(b) indicating the reasons for the proposed revocation;
(c) inviting that person, within 14 days of the notice, to submit representations in writing as to why the recognition should not be revoked.

(6) The Minister must consider any such representations in deciding whether to revoke the recognition and give the person written notice of his or her decision within 7 days after making it.

(7) The revocation takes effect on the date specified in the notice.

22. Pseudonyms

(1) Certification service providers may, at the request of a particular signatory, indicate in the relevant certificate a pseudonym instead of the signatory's name.

(2) If a pseudonym is indicated pursuant to subsection (1), the certification service provider must, where necessary for the investigation of an offence involving the use of electronic signatures or where otherwise required by law to do so, transfer personal data relating to the signatory.

(3) If personal data is transferred pursuant to subsection (2), the certification service

provider must make a record of the transfer and as soon as possible thereafter give notice to the signatory of the transfer.

23. Liability of authorized certification service provider

(1) By issuing an accredited certificate, an authorized certification service provider is liable to any person who reasonably relied on the certificate for:

(a) the accuracy of all information in the accredited certificate as from the date on which it was issued, unless the authorized certification service provider has stated otherwise in the accredited certificate; and

(b) an assurance that the person identified in the accredited certificate held, at the time the accredited certificate was issued, the signature creation device corresponding to the signature verification device given or identified in the accredited certificate; and

(c) if the authorized certification service provider generates both the signature creation device and the signature verification device, assurance that the two devices function together in a complementary manner;
unless the person who relied on the accredited certificate knows or ought reasonably to have known that the authorization of the certification service provider has been revoked.

(2) An authorized certification service provider is not liable for errors in the information in an accredited certificate where:

(a) the information was provided by or on behalf of the person identified in the accredited certificate; and

(b) the certification service provider can demonstrate that all reasonably practical measures have been taken to verify that information.

(3) An authorized certification service provider that:

(a) indicates in the accredited certificate limits on the uses of that certificate; and

(b) makes those limits known to third parties,

is not liable for damages arising from the use of the accredited certificate contrary to those limits.

(4) The limits in subsection (3) may include a limit on the value of transactions for which the accredited certificate is valid.

PART 5 – ENCRYPTION AND DATA PROTECTION

24. Encryption

(1) The Minister may make regulations:

(a) in relation to the use, import and export of encryption programs or other encryption products; and

(b) prohibiting the export of encryption programs or other encryption products from Vanuatu generally or subject to such restrictions as may be prescribed.

(2) For the avoidance of doubt, but subject to any regulations made under subsection (1), it is lawful in Vanuatu for a person to use any encryption program or other encryption product if it has lawfully come into the possession of that person.

25. Data protection

(1) The Minister may make orders prescribing standards for the processing of personal data, whether or not the personal data originates inside Vanuatu.

(2) The regulations may provide for the following:

(a) the voluntary registration and de-registration to the standards by data controllers and data processors;

(b) the establishment of a register that is available for public inspection showing particulars of data controllers and data processors who have registered or de-registered to the standards and the dates thereof and the countries in respect of which the registration applies;

(c) the application of the standards to those countries specified in the regulations;

(d) different standards to be applied in respect of personal data originating from different countries.

(3) A data controller or data processor who voluntarily registers to a standard in subsection (1) must comply with the standard, as it may be amended from time to time, in respect to any personal data that:
(a) originates from a country to which the standard applies; and
(b) is collected by the data controller during the period of registration, including any time after de-registration.

(4) A data controller who fails to comply with subsection (3) is guilty of an offence punishable on conviction by a fine not exceeding VT 1,000,000 or imprisonment for a term not exceeding 6 months, or both.

PART 6 – INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS

26. Liability of intermediaries

(1) An intermediary is not subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary provides services if the intermediary was not the originator of that electronic record and the intermediary:

(a) has no actual knowledge that the information gives rise to civil or criminal liability; or

(b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or

(c) follows the procedure set out in section 27 if the intermediary:
(i) acquires knowledge that the information gives rise to civil or criminal liability; or
(ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

(2) An intermediary is not required to monitor any information contained in an electronic record in respect of which the intermediary provides services in order to establish knowledge of, or to become aware of, facts or circumstances to determine whether or not the information gives rise to civil or criminal liability.

(3) Nothing in this section relieves an intermediary from complying with any contractual or other legal obligation in respect of an electronic record.

27. Procedure for dealing with unlawful, defamatory etc. information

(1) If an intermediary has actual knowledge that the information in an electronic record gives rise to civil or criminal liability, the intermediary must as soon as practicable:

(a) remove the information from any information processing system within the intermediary's control and cease to provide or offer to provide services in respect of that information; and

(b) notify the Minister or appropriate law enforcement agency of the relevant facts and of the identity of the person for whom the intermediary was supplying services in respect of the information, if the identity of that person is known to the intermediary.

(2) If an intermediary is aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information in an electronic record ought reasonably to have been known, the intermediary must as soon as practicable:

(a) follow the relevant procedure set out in a code of conduct or standard approved under section 28 if such code or standard applies to the intermediary; or

(b) notify the Minister.

(3) If the Minister is notified in respect of any information under subsection (2), the Minister may direct the intermediary to:

(a) remove the electronic record from any information processing system within the control of the intermediary; and

(b) cease to provide services to the person to whom the intermediary was supplying services in respect of that electronic record; and

(c) cease to provide services in respect of that electronic record.

(4) An intermediary is not liable (whether in contract, tort, under statute or pursuant to any other right) to any person, including any person on whose behalf the intermediary provides services in respect of information in an electronic record, for any action:
(a) the intermediary takes in good faith under subsection (1); or
(b) as directed by the Minister under subsection (3).

28. Codes of conduct and standards for intermediaries and e-commerce service providers

(1) If the Minister is satisfied that a body or organization represents intermediaries or e-commerce service providers, the Minister may, by notice given to the body or organization, request that body or organization to:

(a) develop a code of conduct that applies to intermediaries or e-commerce service providers and that deals with one or more specified matters relating to the provision of services by those intermediaries or e-commerce service providers; and

(b) provide a copy of that code of conduct to the Minister within such time as may be

specified in the request.

(2) If the Minister is satisfied with the code of conduct provided under subsection (1), the Minister is to approve the code of conduct by notice published in the Gazette. Upon publication, the code of conduct applies to intermediaries or e-commerce service providers as may be specified in the notice.

(3) If the Minister is satisfied that:

(a) no body or organization represents intermediaries or e-commerce service providers; or

(b) a body or organization to which notice is given under subsection (1) has not complied with the request of the Minister under that subsection;
the Minister may, by notice published in the Gazette, approve a standard that applies to intermediaries or e-commerce service providers.

(4) A code of conduct or standard approved under this section may relate to one or more of the following matters:

(a) the types of services and customers that are permitted to be provided services by intermediaries;

(b) the types of information permitted to be contained in electronic records for which services are provided by intermediaries;

(c) the contractual application of relevant codes of conduct or standards to customers of intermediaries and e-commerce service providers;

(d) information to be disclosed by intermediaries and e-commerce service providers including name, address, e-mail address and contact and registration details;

(e) the use of a quality accreditation mark associated with Vanuatu;

(f) the actions to be taken in the event of customers of intermediaries or e-commerce service providers sending bulk, unsolicited electronic records;

(g) business activities carried out electronically by companies under the Companies Act [Cap. 191] or the International Companies Act [Cap. 222] which are prohibited under that Act;

(h) publication of material that contravenes any Act in Vanuatu;

(i) procedures for dealing with complaints;

(j) procedures for dispute resolution, including dispute resolution by electronic means.

29. Offence to contravene code of conduct or standard

(1) If a code of conduct or a standard is approved by the Minister under section 28 to apply to intermediaries or e-commerce service providers, those intermediaries or e-commerce service providers must comply with the code of conduct or standard.

(2) If an intermediary or e-commerce service provider fails to comply with an approved code of conduct or standard, the Minister:

(a) must in the first instance give a written warning to the person; and
(b) may direct the person to cease or otherwise to correct the person's practices.

(3) If a person fails to cease or otherwise correct the person's practices within such period as may be specified in a direction given under subsection (2)(b), the person is guilty of an offence punishable on conviction by a fine not exceeding VT 100,000 for each day on which the contravention continues.

PART 7 – GENERAL

30. Regulations

(1) The Minister may make regulations prescribing all matters:

(a) required or permitted by this Act to be prescribed; or

(b) necessary or convenient to be prescribed for carrying out or giving effect to this Act.

(2) The regulations may prescribe penalties for offences against the regulations. A penalty must not exceed VT 50,000.