ELECTRONIC TRANSACTIONS ACT 2023

Act No. xx of 2023

I assent

Sir …

Governor-General

Dated xxx xx 2023

AN ACT TO PROVIDE FOR THE USE OF ELECTRONIC TRANSACTIONS AND OF ELECTRONIC TRANSFERABLE RECORDS AND TO PROVIDE FOR MATTERS CONNECTED THEREWITH.

ENACTED BY THE PARLIAMENT OF TUVALU
Commencement [Date appointed by the Minister]

**Part 1: Preliminary**

**1. Short Title**

This Act may be cited as the Electronic Transactions Act 2023.

**2. Commencement**

This Act shall come into force on a date appointed by the Minister.

**3. Interpretation**

1. In the interpretation of this Act, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

2. Questions concerning matters governed by this Act which are not expressly settled in it are to be settled in conformity with the general principles on which this Act is based.

Source: MLEC art. 3; ECC art. 5

**4. Definitions**

In this Act, unless the context otherwise requires –

(a) “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;

(b) “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 natural person each time an action is initiated or a response is generated by the system;

(c) “Certificate” means a data message or other record confirming the link between a signatory and signature creation data;

(d) “Certification service provider” means a person that issues certificates and may provide other services related to electronic signatures;

(e) “Communication” means any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, that the parties are required to make or choose to make;

(f) “Data message” means information generated, sent, received or stored by electronic, magnetic, optical or similar means, including, where appropriate, all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not;

(g) “Electronic communication” means any communication that the parties make by means of data messages;

(h) “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 intention in respect of the information contained in the data message;

(i) “Electronic transferable record” is an electronic record that complies with the requirements of section 44;

(j) “Information system” means a system for generating, sending, receiving, storing or otherwise processing data messages;

(k) “Intermediary”, with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message;

(l) “Minister” means the Minister responsible, from time to time, for Trade;

(m) “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;

(n) “Place of business” means any place where a party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location;

(o) “Relying party” means a person who acts on the basis of the result of trust services;

(p) “Signatory” means a person that holds signature creation data and acts either on its own behalf or on behalf of the person it represents.

(q) “Subscriber” means a person who enters into an arrangement for the provision of identity management services or trust services with an identity management service provider or a trust service provider;

(r) “Transferable document or instrument” means a document or instrument issued on paper that entitles the holder to claim the performance of the obligation indicated in the document or instrument and to transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument.”

(s) “Trust service” means an electronic service that provides assurance of certain qualities of a data message and includes the methods for creating and managing electronic signatures, electronic seals, electronic time stamps, website authentication, electronic archiving and electronic registered delivery services;

(t) “Trust service provider” means a person who enters into an arrangement for the provision of one or more trust services with a subscriber.

**5. Crown to be bound**

This Act binds the Crown.

**6. Purpose**

The purpose of this Act is to –

(a) facilitate electronic communications and transactions by means of reliable data messages;

(b) promote business and community confidence in the use of electronic transactions;

(c) facilitate electronic commerce, to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(d) facilitate electronic filing of documents with public agencies, and to promote efficient delivery by public agencies of services by means of reliable data messages;

(e) minimise the incidence of forged data messages, intentional and unintentional alteration of data messages, and fraud in electronic commerce and other electronic transactions;

(f) implement the United Nations Convention on the Use of Electronic Communications in International Contracts and to make the law of Tuvalu on electronic transactions consistent with the provisions of that Convention; and

(g) enable the use of electronic transferable records issued or used in Tuvalu or abroad.

**Part 2: General provisions**

**7. Application**

1. This law applies to any kind of information in the form of data message.

2. This law does not override any legal provision intended for the protection of consumers.

**8. Exclusions**

1. This law does not apply to:

(a) transactions on a regulated exchange;

(b) foreign exchange transactions;

(c) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments;

(d) the transfer of security rights in sale, loan or holding of or agreement to repurchase securities or other financial assets or instruments held with an intermediary.

2. This law does not apply to:

(a) the creation or execution of a will;

(b) the sale or other disposition of immovable property, or any interest in such property.

Source: ECC art. 2

**9. Legal recognition of data messages**

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. Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

3. Nothing in this Act requires a party to use or accept data messages, but a party’s agreement to do so may be inferred from the party’s conduct.

Source: MLEC art. 5 and art. 5 bis; ECC art. 8(2).

**10. Party autonomy**

The provisions in this Act, except sections 18—20, 31—36, 44 and 45, may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under other law.

**11. Information requirements**

Nothing in this Act affects the application of any legal provision 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, incomplete or false statements in that regard.

Source: ECC art. 7

**12. Location of the parties**

1. For the purposes of this Act, a party’s place of business is presumed to be the location indicated by that party, unless another party demonstrates that the party making the indication does not have a place of business at that location.

2. If a party has not indicated a place of business and has more than one place of business, then the place of business for the purposes of this law is that which has the closest relationship to the underlying transaction, having regard to the circumstances known to or contemplated by the parties at any time before or at the time of carrying out that transaction or, where there is no underlying transaction, the principal place of business.

3. If a natural person does not have a place of business, reference is to be made to the person’s habitual residence.

4. A location is not a place of business merely because that is:

(a) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

(b) where the information system may be accessed by other parties.

5. The sole fact that a party makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

Source: ECC art. 6

**13. Time and place of dispatch and receipt of data messages**

1. The time of dispatch of a data message 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 data message 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 data message is received.

2. The time of receipt of a data message 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 a data message 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 data message has been sent to that address. A data message is presumed to be capable of being retrieved by the addressee when it reaches the addressee’s electronic address.

3. A data message 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, as determined in accordance with section 12.

4. Subsection 2 applies notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the data message is deemed to be received under subsection 3.

Source: ECC art. 10.

*Comment: reference is made to “data message” instead of “electronic communication” to facilitate the use of this provision in a non-contractual framework (e.g., in B2G and C2G transactions). Similar considerations apply to the following sections.*

**14. Recognition by parties of data messages**

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.

Source: MLEC art. 12.

**15. Attribution of data messages**

(1) Unless otherwise agreed between the purported originator and the addressee of an electronic communication, the purported originator of the electronic communication is bound by that communication only if the communication was sent by the purported originator or with the authority of the purported originator.

(2) Subsection (1) is not intended to affect the operation of a law (whether written or unwritten) that makes provision for:

(a) conduct engaged in by a person within the scope of the person’s actual or apparent authority to be attributed to another person; or

(b) a person to be bound by conduct engaged in by another person within the scope of the other person’s actual or apparent authority.

Source: s 15 Australian ETA (simplifies MLEC art. 13).

**16. Acknowledgement of receipt**

(1) Subsections (2) to (4) apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where 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, sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(4) Where the originator has not stated that the data message 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 data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee’s acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

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

Source: MLEC art. 14.

**17. Admissibility and evidential weight of data messages**

1. In any legal proceedings, nothing in the application of the rules of evidence 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, regard shall be had 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.

Source: MLEC art. 9.

**Part 3 Functional Equivalence**

**18. Writing**

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. Subsection (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.

Sources: MLEC art. 6

**19. Original**

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 made available, that information is capable of being displayed to the person to whom it is to be made available.

2. Subsection (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 paragraph (a) of subsection (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.

Source: MLEC art. 8.

*Comment: Subsection 1(b) contains the words “made available” from art. 9(4)(b) ECC.*

**20. Retention of data messages**

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 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, provided that the conditions set forth in paragraphs (a), (b) and (c) of subsection (1) are met.

Source: MLEC art. 10.

**Part 4: Contracts in Electronic Form**

**21. Formation and validity of contracts**

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 electronic communications. Where an electronic communication is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that an electronic communication was used for that purpose.

Source: MLEC art. 11.

*Comment: replaces “data message” (referred to in MLEC) with “electronic communication” as the notion of “electronic communication” is more directly relevant to contracts.*

**22. Invitations to make offers**

A proposal to form 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.

Source: ECC art. 11.

*Comment: applies, for instance, to offers made to the public contained in webpages.*

**23. Use of automated message systems**

A contract formed or performed, in part or in full, 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 or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

Source: ECC art. 12

*Comment: original provision has been complemented with a reference to contract performance.*

**24. Availability of contract terms**

Nothing in this Act 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 which contain the contractual terms in a particular manner, or relieves a party from the legal consequences of its failure to do so.

Source: ECC art. 13.

**25. Error in electronic communications**

1. Where a natural person makes an input error in an electronic communication exchanged with the automated message system of another party and the automated message system does not provide the person with an opportunity to correct the error, that person, or the party on whose behalf that person was acting, has the right to withdraw the portion of the electronic communication in which the input error was made if:

(a) the person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned of the error and indicates that he or she made an error in the electronic communication; and

(b) the person, or the party on whose behalf that person was acting, has not used or received any material benefit or value from the goods or services, if any, received from the other party.

2. Nothing in this section affects the application of any rule of law that may govern the consequences of any error other than as provided for in subsection 1.

Source: ECC art. 14.

**Part 5: Electronic Signatures and Trust Services**

**26. Technology neutrality**

Nothing in this Act, except section 10, shall be applied so as to exclude, restrict or deprive of legal effect any method used in electronic signatures and trust services that satisfies the requirements of this Part or otherwise meets the requirements of applicable law.

Source: MLES art. 3.

*Comment: source texts has been modified to refer to trust services. The last words refer to instances when higher security requirements are required in other acts.*

**27. Relationship with other law**

1. Nothing in this Act affects a legal requirement that a person be identified or that a trust service be used in accordance with a procedure defined or prescribed by law.

2. Other than as provided for in this Act, nothing in this Act affects the application to trust services of any law applicable to data privacy and protection.

Source: MLIT art. 2(3) and (4)

**28. Legal recognition of trust services**

The result deriving from the use of a trust service shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that:

 (a) it is in electronic form; or

 (b) the trust service is not designated pursuant to section 38.

Source: MLIT art. 13

**29. Obligations of trust service providers**

1. A trust service provider shall, at a minimum:

(a) have in place operational rules, policies and practices, including a plan to ensure continuity in case of termination of activity, as appropriate to the purpose and design of the trust service;

 (b) act in accordance with its operational rules, policies and practices, and any representations that it makes with respect to them;

 (c) make its operational rules, policies and practices easily accessible to subscribers, relying parties and other third parties;

 (d) provide and make publicly available means by which a subscriber may notify the trust service provider of a security breach pursuant to section 30; and

 (e) provide easily accessible means that enable a relying party to ascertain, where relevant:

(i) any limitation on the purpose or value for which the trust service may be used; and

(ii) any limitation on the scope or extent of liability stipulated by the trust service provider.

2. If a breach of security or loss of integrity occurs that has a significant impact on a trust service, the trust service provider shall in accordance with the law:

 (a) take all reasonable steps to contain the breach or loss, including, where appropriate, suspending or revoking the affected service;

 (b) remedy the breach or loss; and

 (c) notify the breach or loss.

Source: MLIT art. 14

*Comment: subsection 3 does not need to be enacted if there is a corresponding provision in the data protection law.*

**30. Obligations of subscribers**

The subscriber shall notify the trust service provider, by utilising means made available by the trust service provider pursuant to subsection 1 of section 29 or by otherwise using reasonable means, if:

 (a) the subscriber knows that data or means used by the subscriber for access and usage of the trust service has been compromised; or

 (b) the circumstances known to the subscriber give rise to a substantial risk that the trust service may have been compromised.

Source: MLIT art. 15

*Comment: section 30 does not need to be enacted if there is a corresponding provision in the data protection law.*

**31. Electronic signatures**

Where the law requires a signature of a person, or provides consequences for the absence of a signature, that requirement is met in relation to a data message if a reliable method in accordance with subsection 1 of section 37, or subsection 4 of section 37, is used:

(a) to identify the person; and

(b) to indicate the person’s intention in respect of the information contained in the data message.

Source: MLIT art. 16

**32. Electronic seals**

Where the law requires a person to affix a seal, or provides consequences for the absence of a seal, that requirement is met in relation to a data message if a reliable method in accordance with subsection 1 of section 37, or subsection 4 of section 37, is used:

(a) to provide reliable assurance of the origin of the data message; and

(b) to detect any alteration to the data message after the time and date of affixation, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display.

Source: MLIT art. 17

*Comment: electronic seals may be affixed by physical and legal persons*

**33. Electronic timestamps**

Where the law requires a document, record, information or data to be associated with a time and date, or provides consequences for the absence of a time and date, that requirement is met in relation to a data message if a reliable method in accordance with subsection 1 of section 37, or subsection 4 of section 37, is used:

(a) to indicate the time and date, including by reference to the time zone; and

 (b) to associate that time and date with the data message.

Source: MLIT art. 18

**34. Electronic archiving**

Where the law requires a document, record or information to be retained, or provides consequences for the absence of retention, that requirement is met in relation to a data message if a reliable method in accordance with subsection 1 of section 37, or subsection 4 of section 37, is used:

(a) to make the information contained in the data message accessible so as to be usable for subsequent reference;

 (b) to indicate the time and date of archiving and associate that time and date with the data message;

 (c) to retain the data message in the format in which it was generated, sent or received, or in another format which can be demonstrated to detect any alteration to the data message after that time and date, apart from the addition of any endorsement and any change that arises in the normal course of communication, storage and display; and

 (d) to retain such information, if any, as enables the identification of the origin and destination of a data message and the time and date when it was sent or received.

Source: MLIT art. 19

**35. Electronic registered delivery services**

Where the law requires a document, record or information to be delivered by registered mail or similar service, or provides consequences for the absence of delivery, that requirement is met in relation to a data message if a reliable method in accordance with subsection 1 of section 37, or subsection 4 of section 37, is used:

(a) to indicate the time and date when the data message was received for delivery and the time and date when it was delivered;

 (b) to detect any alteration to the data message after the time and date when the data message was received for delivery to the time and date when it was delivered, apart from the addition of any endorsement or information required by this section, and any change that arises in the normal course of communication, storage and display; and

 (c) to identify the sender and the recipient.

Source: MLIT art. 20

**36. Website authentication**

Where the law requires website authentication, or provides consequences for the absence of website authentication, that requirement is met if a reliable method in accordance with subsection 1 of section 37, or subsection 4 of section 37, is used:

(a) to identify the person who holds the domain name for the website; and

(b) to associate that person to the website.

Source: MLIT art. 21

**37. Reliability requirements for trust services**

1. For the purposes of sections 31 to 36, the method shall be:

(a) as reliable as appropriate for the purpose for which the trust service is being used; or

 (b) deemed to be as reliable as appropriate if proven in fact by or before a court or competent adjudicative body to have fulfilled the functions described in the section, by itself or together with further evidence.

2. In determining the reliability of the method, all relevant circumstances shall be taken into account, which may include:

 (a) compliance of the trust service provider with the obligations listed in section 29;

 (b) compliance of the operational rules, policies and practices of the trust service provider with any applicable recognised international standards and procedures relevant for the provision of trust services;

 (c) any relevant level of reliability of the method used;

 (d) any applicable industry standard;

 (e) the security of hardware and software;

 (f) financial and human resources, including existence of assets;

 (g) the regularity and extent of audit by an independent body;

 (h) the existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;

 (i) the purpose for which the trust service is being used; and

 (j) any relevant agreement between the parties, including any limitation on the purpose or value of the transactions for which the trust service might be used.

3. In determining the reliability of the method, no regard shall be had:

 (a) to the geographic location where the trust service is provided; or

 (b) to the geographic location of the place of business of the trust service provider.

4. A method used by a trust service designated pursuant to section 38 is presumed to be reliable.

5. Subsection 4 does not limit the ability of any person:

 (a) to establish in any other way the reliability of a method; or

 (b) to adduce evidence of the non-reliability of a method used by a trust service designated pursuant to section 38.

Source: MLIT art. 22

**38. Designation of reliable trust services**

1. The Minister may designate trust services that are presumed reliable.

2. The Minister shall:

 (a) take into account all relevant circumstances, including the factors listed in section 37, in designating a trust service; and

 (b) publish a list of designated trust services, including details of the trust service provider.

3. Any designation pursuant to subsection 1 shall be consistent with recognised international standards and procedures relevant for performing the designation process.

4. In designating a trust service, no regard shall be had:

 (a) to the geographic location where the trust service is provided; or

 (b) to the geographic location of the place of business of the trust service provider.

Source: MLIT art. 23

**39. Liability of trust service providers**

1. The trust service provider shall be liable for loss caused to the subscriber or to the relying party due to a failure to comply with its obligations under section 29.

2. Subsection 1 shall be applied in accordance with rules on liability under the law and is without prejudice to:

 (a) any other basis of liability under the law, including liability for failure to comply with contractual obligations; or

 (b) any other legal consequences of a failure of the trust service provider to comply with its obligations under this Law.

3. Notwithstanding subsection 1, the trust service provider shall not be liable to a subscriber for loss arising from the use of a trust service to the extent that:

 (a) that use exceeds the limitations on the purpose or value of the transaction for which the trust service is used; and

 (b) those limitations are contained in the arrangement between the trust service provider and the subscriber.

4. Notwithstanding subsection 1, the trust service provider shall not be liable to a relying party for loss arising from the use of a trust service to the extent that:

 (a) that use exceeds the limitations on the purpose or value of the transaction for which the trust service is used; and

 (b) the trust service provider has complied with its obligations under subsection 1, paragraph (e) of section 29 with respect to that transaction.

Source: MLIT art. 24

**40. Cross-border recognition of the result of the use of trust services**

1. The result deriving from the use of a trust service provided outside Tuvalu shall have the same legal effect in Tuvalu as the result deriving from the use of a trust service provided in Tuvalu if the method used by the trust service offers:

 (a) at least an equivalent level of reliability, where the reliability levels recognised by such jurisdictions are identical; or

 (b) substantially equivalent or higher level of reliability, in all other cases.

2. For the purposes of determining satisfaction of subsection 1, regard shall be had to recognised international standards.

3. The trust service shall be presumed to satisfy subsection 1 if the Minister has determined the equivalence, taking into account subsection 2 of section 37.

4. Where, notwithstanding subsections 2, 3 and 4, parties agree, as between themselves, to the use of certain types of trust services, that agreement shall be recognised as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

Source: MLIT art. 26; subsection 4 derives from MLES art. 12(5)

**Part 6: Electronic Transferable Records**

**41. Electronic Transferable Records**

1. Other than as provided for in this Part, nothing in this Act affects the application to an electronic transferable record of any rule of law governing a transferable document or instrument including any rule of law applicable to consumer protection.

2. This Part does not apply to securities, such as shares and bonds, and other investment instruments.

Source: MLETR art. 1

**42. Legal Recognition of an Electronic Transferable Record**

An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it is in electronic form.

Source: MLETR art. 7

**43. Additional information in electronic transferable records**

Nothing in this Law precludes the inclusion of information in an electronic transferable record in addition to that contained in a transferable document or instrument.

Source: MLETR art. 6

**44. Transferable Documents or Instruments**

1. Where the law requires a transferable document or instrument, that requirement is met by a data message if:

(a) The data message contains the information that would be required to be contained in a transferable document or instrument; and

 (b) A reliable method is used:

(i) to identify that data message as the electronic transferable record;

(ii) to render that data message capable of being subject to control from its creation until it ceases to have any effect or validity; and

(iii) to retain the integrity of that data message.

2. The criterion for assessing integrity shall be whether information contained in the electronic transferable record, including any authorised change that arises from its creation until it ceases to have any effect or validity, has remained complete and unaltered apart from any change which arises in the normal course of communication, storage and display.

Source: MLETR art. 10

**45. Control**

1. Where the law requires or permits the possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used:

 (a) to establish exclusive control of that electronic transferable record by a person; and

 (b) to identify that person as the person in control.

2. Where the law requires or permits transfer of possession of a transferable document or instrument, that requirement is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record.

Source: MLETR art. 11

**46. Indication of Time and Place in Electronic Transferable Records**

Where the law requires or permits the indication of time or place with respect to a transferable document or instrument, that requirement is met if a reliable method is used to indicate that time or place with respect to an electronic transferable record.

Source: MLETR art. 13

**47. Endorsement**

Where the law requires or permits the endorsement in any form of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if the information required for the endorsement is included in the electronic transferable record and that information is compliant with the requirements set forth in sections 18 and 31.

Source: MLETR art. 15

**48. Amendment**

Where the law requires or permits the amendment of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if a reliable method is used for amendment of information in the electronic transferable record so that the amended information is identified as such.

Source: MLETR art. 16

**49. Replacement of a Transferable Document or Instrument with an Electronic Transferable Record**

1. An electronic transferable record may replace a transferable document or instrument if a reliable method for the change of medium is used.

2. For the change of medium to take effect, a statement indicating a change of medium shall be inserted in the electronic transferable record.

3. Upon issuance of the electronic transferable record in accordance with subsections 1 and 2, the transferable document or instrument shall be made inoperative and ceases to have any effect or validity.

4. A change of medium in accordance with subsections 1 and 2 shall not affect the rights and obligations of the parties.

Source: MLETR art. 17

**50. Replacement of an Electronic Transferable Record with a Transferable Document or Instrument**

1. A transferable document or instrument may replace an electronic transferable record if a reliable method for the change of medium is used.

2. For the change of medium to take effect, a statement indicating a change of medium shall be inserted in the transferable document or instrument.

3. Upon issuance of the transferable document or instrument in accordance with subsections 1 and 2, the electronic transferable record shall be made inoperative and ceases to have any effect or validity.

4. A change of medium in accordance with subsections 1 and 2 shall not affect the rights and obligations of the parties.

Source: MLETR art. 18

**51. General Reliability Standard**

For the purposes of sections 44, 45, 46, 48, 49 and 50, the method referred to shall be:

 (a) as reliable as appropriate for the fulfilment of the function for which the method is being used, in light of all relevant circumstances, which may include:

(i) any operational rules relevant to the assessment of reliability;

(ii) the assurance of data integrity;

(iii) the ability to prevent unauthorised access to and use of the system;

(iv) the security of hardware and software;

(v) the regularity and extent of audit by an independent body;

(vi) the existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method;

(vii) any applicable industry standard; or

 (b) proven in fact to have fulfilled the function by itself or together with further evidence.

Source: MLETR art. 12

**52. Non-Discrimination of Foreign Electronic Transferable Records**

1. An electronic transferable record shall not be denied legal effect, validity or enforceability on the sole ground that it was issued or used abroad.

2. Nothing in this Part affects the application to electronic transferable records of rules of private international law governing a transferable document or instrument.

Source: MLETR art. 19

**Part 7 – Miscellaneous**

**53. Regulations under this Act**

The Minister may make Regulations —

(a) prescribing modalities for the application of this Act to public bodies, in cooperation with the concerned body;

(b) prescribing forms and fees required under this Act; and

(c) for the proper and efficient administration of this Act.