

**THE REPUBLIC OF KIRIBATI**



**ELECTRONIC TRANSACTIONS ACT 2021**

**Arrangement of Sections**

**PART 1 – PRELIMINARY**

1. Short Title
2. Commencement
3. Definitions
4. Objective of the Act
5. Administration of the Act
6. Republic to be bound
7. Exclusions and general power of Minister to exclude and include matters under Act
8. Voluntary use of computer data

**PART 2 – LEGAL RECOGNITION OF ELECTRONIC COMMUNICATIONS**

9. Legal recognition of computer data and electronic communications
10. Writing
11. Admissibility and evidential weight of computer data and electronic communications
12. Legal requirement to retain information
13. Producing and retaining electronic versions of paper-based documents or records
14. Time and place of dispatch and receipt of electronic communications
15. Determining place of business

**PART 3 – ELECTRONIC CONTRACTING**

16. Attribution of electronic communications
17. Formation and validity of contracts
18. Invitations to make offers
19. Use of automated message systems for contract formation
20. Availability of contract terms
21. Error in electronic communications

#### **PART 4- ELECTRONIC SIGNATURES**

- 22. Equal treatment of signature technologies
- 23. Legal requirement for a signature

#### **PART 5- ELECTRONIC TRANSFERABLE RECORDS**

- 24. Application of this Part
- 25. Additional information in electronic transferable records
- 26. General reliability standard
- 27. Legal requirement for an electronic transferable record
- 28. Control
- 29. Indication of time and place in electronic transferable record
- 30. Endorsement
- 31. Amendment
- 32. Replacement of a transferable document or instrument with an electronic transferable record
- 33. Replacement of an electronic transferable record with a transferable document or instrument
- 34. Non-discrimination of foreign electronic transferable records

#### **PART 6- ELECTRONIC EXCHANGES WITH PUBLIC BODIES**

- 35. Authorization for public bodies to use computer data and electronic signatures

#### **PART 7- MISCELLANEOUS**

- 36. Rules governing electronic evidence
- 37. Powers to make Regulations

THE REPUBLIC OF KIRIBATI



(No of 2021)



I assent,

A handwritten signature in black ink, appearing to be 'Beretitenti'.

Beretitenti

21/02/2021

AN ACT

entitled

**AN ACT TO GIVE LEGAL EFFECT TO ELECTRONIC TRANSACTIONS,  
CONTRACTING, SIGNATURES AND FOR OTHER CONNECTED PURPOSES**

Commencement date:

MADE by the Maneaba ni Maungatabu and assented to by the Beretitenti

**PART I - PRELIMINARY**

**1 Short title**

This Act may be cited as the Electronic Transactions Act 2021.

**2. Commencement**

This Act commences on a date that the Minister may by notice appoint.

### 3. Definitions

In this Act, unless the context otherwise requires —

“addressee” of a computer data means a person who is intended by the originator to receive the computer data, but does not include a person acting as an intermediary with respect to that computer data;

“automated message system” means a computer program or an electronic or other automated means used to initiate an action or respond to computer data 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;

“computer data” 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 computer data, whether generated contemporaneously or not;

“electronic communication” means any statement, declaration, demand, notice or request, including an offer and the acceptance of an offer, made by using computer data;

“electronic signature” means data in electronic form in, affixed to or logically associated with, computer data, which may be used to identify the signatory in relation to the computer data and to indicate the signatory’s intention in respect of the information contained in the computer data;

“electronic transferable record” means computer data that complies with the requirement of section 27;

“information system” means a system for generating, sending, receiving, storing or otherwise processing computer data;

“intermediary” with respect to particular computer data, means a person who, on behalf of another person, sends, receives or stores that computer data or provides other services with respect to that computer data;

“originator” of computer data means a person by whom, or on whose behalf, the computer data has been sent or generated prior to storage, if any, but it does not include a person acting as intermediary with respect to that computer data;

“transferable document or instrument” means a document or instrument issued on paper that entitles the holder to;

(a). claim the performance of the obligation indicated in the document or instrument;  
and

(b). transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument;

#### **4. Objective of the Act**

The objectives of the Act are to:

- (a). to recognise the validity of and promote the development of electronic communications in commercial and non-commercial dealings and in dealings with governmental entities;
- (b). facilitate electronic communications by means of reliable **electronic records**;
- (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 communication;
- (d). facilitate electronic filing of documents with public authorities, and to promote efficient delivery of ICT services by Government entities by means of reliable electronic records;
- (e). minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;
- (f). help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records;
- (g). promote public confidence in the integrity and reliability of electronic records and electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium; and
- (h). implement the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the United Nations on 23 November 2005, and to make the law of Kiribati on electronic transactions, whether or not involving parties whose places of business are in different States, consistent with the provisions of that Convention.

#### **5. Administration of the Act**

- (1). This Act shall be administered under the direction and control of the Minister responsible for Commerce and Trade.
- (2). The application of Part 6 of this Act shall be administered under the direction and control of the Minister responsible for Communication and Information.
- (3). The Ministers have power to delegate the administration of this Act to officers within their Ministry.

#### **6. Republic to be bound**

This Act binds the Republic.

**7. Exclusions and General Power of Minister to exclude and include matters under Act**

(1). This Act shall not apply to any written law requiring writing, signatures, or original documents for-

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

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

(2). Notwithstanding subsection (1), the Minister may by Order in writing, make this Act or such provisions as are specified in the order, applicable to any of the legal requirements set out in subsection (1) and to any class of transactions, person, matters or things specified in the order.

**8. Voluntary use of computer data**

Nothing in this Act requires or prohibits;

(a) a person or party to use or accept computer data, including electronic signatures or electronic contracts;

(b) any Ministry, department or agency of the Government to generate, send, receive, store or otherwise process any computer data by electronic means.

**PART 2- LEGAL RECOGNITION OF ELECTRONIC COMMUNICATIONS**

**9. Legal recognition of computer data and electronic communications**

Information shall not be denied legal effect, validity, enforceability, or admissibility

solely on the ground that it is;

(a). in the form of electronic communication or computer data; or

(b). not contained in the electronic communication or computer data purporting to give rise to such legal effect but is merely referred to in that electronic communication or computer data.

**10. Writing**

(1). Any written law that requires or permits information to be in writing is met by computer data, if the information contained in the computer data 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.

**11. Admissibility and evidential weight of computer data and electronic communications**

- (1). In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of any electronic communication or computer data in evidence:
  - (a). on the sole ground that it is an electronic communication or computer data; 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 an electronic communication or computer data shall be given due evidential weight.
- (3). In assessing the evidential weight of any electronic communication or computer data, regard shall be made to:
  - (a). the reliability of the manner in which the electronic communication or computer data was generated, stored or communicated;
  - (b). the reliability of the manner in which the integrity of the information was maintained;
  - (c). the manner in which the originator was identified; and
  - (d). any other relevant factors deemed just to be considered.
- (4). This section shall not affect the application of section 28 of the Evidence Act currently applicable in Kiribati.

**12. Legal requirement to retain information**

- (1). Any written law that requires information to be retained is met by a computer data if:
  - (a). the information contained therein is accessible so as to be usable for subsequent reference;
  - (b). a reliable method is used to retain the integrity of the information from the time when it was first generated in its final form, as a computer data or otherwise; and
  - (c). such information, if any, is retained as enables the identification of the origin and destination of a computer data and the date and time when it was sent or received.
- (2). Subsection (1) applies whether the requirement 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 subsection 1(b):

(a). the criterion 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 method shall be as reliable as is appropriate for the purpose for which the information was generated, in the light of all the relevant circumstances.

**13. Producing and retaining electronic versions of paper-based documents or records**

(1). Subject to Part 6, any written law that requires or permits a document or record issued on paper or in other non-electronic form to be produced to a person is met by a computer data if;

(a) the information contained therein is accessible so as to be usable for subsequent reference;

(b). a reliable method is used to retain the integrity of the information from the time when it was first generated in its final form, as a computer data or otherwise; and

(c) the person consents to the receipt of the computer data.

(2). Subject to Part 6, any written law that requires or permits a document or record issued on paper or in other non-electronic form to be retained is met by a computer data if;

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b). a reliable method is used to retain the integrity of the information from the time when it was first generated in its final form, as a computer data or otherwise.

(3). Subsection (1) and (2) apply whether the requirement is in the form of an obligation or whether the law simply provides for the consequences for the information not being produced or retained in its original form.

(4). For the purposes of subsection 1(b) and 2(b);

(a). the criterion 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 method shall be as reliable as is appropriate for the purpose for which the information was generated, in light of all the relevant circumstances.

**14. Time and place of dispatch and receipt of electronic communications**

(1). The time of dispatch of an electronic communication is:

(a). 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;

(b). 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.

(3). 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 the address and the addressee becomes aware that the electronic communication has been sent to that address.

(4). For the purpose of subsections (2) and (3), an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

(5). 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, as determined in accordance with section 15.

#### **15. Determining place of business**

(1). For the purposes of this Act, a person's place of business is any place where the person maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of good or services out of a specific location.

(2). A person's place of business is presumed to be the location indicated by that party, unless it is demonstrated that the party making the indication does not have a place of business at that location.

(3). If a person has not indicated a place of business and has more than one place of business, the place of business is:

(a). the place of business which has the closest relationship to the underlying transaction;  
or

(b). if there is no underlying transaction, the person's principal place of business.

(4). If a natural person does not have a place of business within the meaning of subsection (1), the person's habitual residence is that person's place of business.

(5). A location is not a place of business merely because that is:

(a). where equipment and technology supporting an information system used by a person are located; or

(b). where the information system may be accessed by another person.

(6). The sole fact that a person makes use of a domain name or electronic mail address connected to a specific country does not create a presumption that the person's place of business is located in that country.

### **PART 3- ELECTRONIC CONTRACTING**

#### **16. Attribution of electronic communications**

As between the originator and the addressee, unless otherwise agreed an electronic communication 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 electronic communication; or

(b). by an information system programmed by, or on behalf of, the originator to operate automatically.

**17. Formation and validity of contracts**

(1). In the context of contract information, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of electronic communications.

(2). If 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.

**18. Invitations to make offers**

A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific persons, but is generally accessible to persons 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 person making the proposal to be bound in case of acceptance.

**19. Use of automated message systems for contract formation**

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 or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

**20. Availability of contract terms**

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

**21. Error in electronic communications**

(1). If:

(a). a natural person makes an input error in electronic communications exchanged with the automated message system of another party; and

(b). the automated message system does not provide the person with an opportunity to correct the error,

the 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.

(2). Subsection (1) does not apply unless the person, or the party on whose behalf that person was acting;

(a). 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). has not used or received any material benefit or value from the goods or services, if any, received from the other party.

(3). Nothing in this section affects the application of any written law that may govern the consequences of any error other than as provided for under subsection (1).

#### **PART 4- ELECTRONIC SIGNATURES**

##### **22. Equal treatment of signature technologies**

Without limiting section 8, nothing in this Act shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies the requirements referred to in section 23(1), or otherwise meets the requirements of applicable law.

##### **23. Legal requirement for a signature**

(1). A written law that requires or permits the signature of a person is met in relation to computer data if:

(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the computer data; and

(b) The method used is either:

(i) as reliable as appropriate for the purpose for which the computer data was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii) proven in fact to have fulfilled the functions described in subsection (a) above, by itself or together with further evidence.

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

(3). In determining the reliability of an electronic signature, no regard shall be had to:

(a). the geographic location where the electronic signature is created or used; or

(b). the geographic location of the place of business of the issuer or signatory.

#### **PART 5- ELECTRONIC TRANSFERABLE RECORDS**

##### **24. Application of this Part**

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

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

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

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

**26. General reliability standard**

(1). For the purpose of this Part, a method shall be deemed reliable if it is:

(a). as reliable as is 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 unauthorized access to and use of the system;

(iv). the security of hardware and software;

(v). the regularity and extent of audit of 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.

**27. Legal requirement for an electronic transferable record**

(1). A written law that requires a transferable document or instrument is met by particular computer data if:

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

(b). a reliable method is used to:

(i). identify that computer data as the electronic transferable record;

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

(iii). retain the integrity of that computer data.

(2). For the purposes of subsection (1) (b) (iii), the criterion for assessing integrity shall be whether information contained in the electronic transferable record, including any authorized 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.

**28. Control**

(1). Any written law that requires or permits the possession of a transferable document or instrument is met with respect to an electronic transferable record if a reliable method is used to:

- (a). establish exclusive control of that electronic transferable record by a person; and
- (b). identify that person as the person in control.

(2). Any written law that requires or permits transfer of possession of a transferable document or instrument is met with respect to an electronic transferable record through the transfer of control over the electronic transferable record.

**29. Indication of time and place in electronic transferable record**

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

**30. Endorsement**

Any written law that requires or permits the endorsement in any form of a transferable document or instrument 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 section 10 and 23.

**31. Amendment**

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

**32. 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 this section, 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 this section shall not affect the rights and obligations of the parties.

**33. 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 this section, the electronic transferable record shall be made inoperative and ceases to have any effect or validity.
- (4). A change of medium in accordance with this section shall not affect the rights and obligations of the parties.

**34. 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.

**PART 6- ELECTRONIC EXCHANGES WITH PUBLIC BODIES**

**35. Authorisation for public bodies to use computer data and electronic signatures**

- (1). Any public body, that pursuant to any written law;
  - (a). accepts the filing of documents, or obtains information in any form;
  - (b). requires that documents be created or retained;
  - (c). requires documents, records or information to be produced or retained in their original form;
  - (d). issues any permit, license or approval; or
  - (e). requires payment of any fee, charge or other amount by any method and manner of payment;

may notwithstanding anything to the contrary in such written law, carry out that function by means of computer data, including the use of an electronic signature.

- (2). If a public body carries out any of the functions referred to in subsection (1) by means of computer data, the public body may specify:
  - (a). the manner and format in which such computer data shall be generated, sent, received or stored;
  - (b). the type of electronic signature and the manner and format in which the signature shall be affixed to or logically associated with the computer data;

(c). such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of computer data; and

(d). any other required attributes for computer data that are currently specified for corresponding paper documents.

(3). For the avoidance of doubt, notwithstanding anything to contrary in any written law but subject to any specification made under subsection (2), any written law that requires a person to:

(a). provide information to a public body;

(b). generate or store information for a public body;

(c). use a prescribed form for an application or notification to, or other transaction with, a public body;

(d). produce to or retain for a public body any document, record or information in its original form; or

(e). hold a license, permit or other approval from a public body, is met by a computer data specified by the public body for that purpose and-

(i). in the case of a requirement referred to in paragraph (a), (c) and (d) sent or retained (as the case may be) in the manner specified by the public body;

(ii). in the case of a requirement referred to in paragraph (b), generated or retained (as the case may be) in the manner specified by the public body; or

(iii). in the case of a requirement referred to in paragraph (e), issued by the public body.

(4). Nothing in this Act shall by itself compel any public body to generate, send or receive computer data.

## **PART 7- MISCELLANEOUS**

### **36. Rules governing electronic evidence**

(1). Notwithstanding the provisions contained in the Evidence Act or any other written law, the following provisions shall apply to Parts 2, 3, 4, 5 and 6 of this Act, in any civil or legal proceedings.

(2). Any information contained in any computer data, electronic document, electronic record or electronic communication-

(a). touching any fact in issue or relevant fact; and

(b). compiled, received or obtained during the course of any business, trade or profession or other regularly conducted activity;

shall be admissible in any civil proceedings under this Act, provided that direct oral evidence of such fact in issue or relevant matter, if available, shall be admissible; and there is no reason

to believe that the information contained in a computer data, electronic document, electronic record or any electronic communication is unreliable or inaccurate.

(3). The Courts shall, unless the contrary is proved, presume the truth of information contained in a computer data, electronic document, electronic record or electronic communication, and in the case of any computer data, electronic document, electronic record or electronic communication made by a person or government entity, that the said computer data, electronic document, electronic record or electronic communication was made by the person who is purported to have made it and similarly, shall presume the validity of any electronic signature or authentication method or distinctive identification mark therein.

### **37. Power to make Regulations**

(1). The Minister responsible for Commerce and Trade, upon the advice of Cabinet, may make regulations relating to;

(a). the prescribed forms for any application, notice, certificate and other documents required for the purposes of this Act;

(b). any fees applicable under this Act; and

(c). any matter in respect of which the Minister considers necessary or expedient for the effective execution of the provisions of this Act.

(2). The Minister responsible for Communication and Information, upon the advice of Cabinet, may make regulations relating to the same in (a), (b) and (c) but only to Part 6 of this Act.

## Explanatory Memorandum

### **Background and context**

The broader use of information and communication technologies (ICT) is critical to foster economic and social development. ICT benefits are particularly important in small island States given geographical challenges and the shortage of physical infrastructure.

The Asia – Pacific region has been at the forefront of the use of ICT technologies, including in the context of paperless trade facilitation. The pervasive use of ICT is the result of three elements: sound policy decisions, robust network and a legal environment in line with international standards both in the regulatory and in the enabling aspects.

The Investment Policy Framework, the Trade Policy Framework and the ICT Policy 2019 all highlighted the need to create an enabling environment for developing the digital economy. The implementation of those recommendations requires the adoption of relevant legislative framework. In particular, the National ICT Policy 2019, paragraph 6.4, requires the adoption of a modern enabling environment for the use of electronic communications. The adoption of this Act has also been recommended in the UNCTAD Rapid eTrade Readiness Assessment of Kiribati. The Government also acceded the Electronic Communications Convention in 2019.

Several pieces of legislation are relevant to enable fully the use of electronic means. Of all possible relevant laws, the foundational one is the law on electronic transactions and signatures. Those foundation rules are contained in the Electronic Transactions Act.

### **Scope of application**

The Electronic Transactions Act provides legal recognition and status to the use of electronic communications and signatures. It applies to all types of electronic transactions – i.e., those exchanged among business, government and citizens/consumers – subject to the consent of the concerned persons. Application of the Act to transactions with public bodies is subject to the issuance of implementing regulations according to section 35. This comprehensive approach reflects the cross-cutting nature of electronic transactions, which are relevant for every field of economic activity as well as for an increasing number of social activities.

The Electronic Transactions Act enables the use of electronic means by removing legal obstacles and illustrating the requirements under which paper-based and electronic communications and documents are considered equivalent. It does not amend in any manner existing legislation.

One major effect of the adoption of an Electronic Transactions Act is to legally validate all business-to-business and business-to-consumer electronic exchanges. Such Act will also provide a legal framework for paperless trade facilitation and national single window operations.

Reflecting the cross-cutting nature of electronic transactions, the Act is overall administered under the direction and control of the Minister responsible for Commerce and Trade. However, the application of **Part 6** of this Act, relating to exchanges of electronic transactions with public bodies, is administered under the direction and control of the Minister responsible for Communication and Information, which is in charge of e-Government matters (**section 5**).

The Act has also been reviewed to ensure compatibility with the Cybercrime Act.

## **Structure and content**

The Act is based on the model laws prepared by the United Nations Commission on International Trade Law (UNCITRAL). UNCITRAL is the core legal body of the United Nations for preparing laws and conventions enabling trade. UNCITRAL texts on electronic transactions have been adopted in more than 100 States, and they are in force in all Pacific States that have adopted electronic transactions laws: Australia, Fiji, New Zealand, Samoa, Tonga and Vanuatu. UNCITRAL texts are also referenced in major regional free trade agreements such as CPTPP and RCEP, which makes the Electronic Transactions Act future-proof.

UNCITRAL drafted also the United Nations Convention on the Use of Electronic Communications in International Contracts (ECC), which is in force in Kiribati and deals with cross-border aspects of electronic transactions. The ECC and the Electronic Transactions Act are therefore complementary, and accordingly one goal of the Act is to implement that Convention.

**Part 1** of the Act deals with objective, scope and other general matters. The main goal of the Act is to provide legal recognition to the use of electronic transactions. The Act applies to all types of electronic transactions. However, its application to exchanges with public bodies (e-Government) is subject to the adoption of implementing regulations (section 35).

The definitions in section 3 are taken from UNCITRAL texts (see table below for details). The only exception is the definition of “computer data”, which usually corresponds to the defined term “data message”. The change has been made at the request of OAG to ensure consistency with the Cybercrime Act. In any case, “computer data” in this Act should be understood in the same sense as “data message” in UNCITRAL texts and their enactments.

Electronic transactions are used in all human activities. Their main fields of application are in commercial operations (business to business and business to consumer) and in transactions with public bodies (e-Government). According to the general distribution of competencies in Government, the Act gives competence to administer the Act (section 5) and to adopt the relevant regulations (sections 35 and 37) to the Minister responsible for Communication and Information with respect to e-Government matters, and to the Minister responsible for Commerce and Trade for all other matters.

In particular, the Minister responsible for Commerce and Trade maintains competence for the implementation of the national single window system and other paperless trade facilitation initiatives. The passing of the Act is critical to clarify the legal status of these initiatives, which need to be carried out online.

The only matters excluded from the scope of application of the Acts are wills and transfer of real estate rights (section 7(1)). These exclusions are in line with prevailing international practice. The Minister may review the list of exclusions in light of the practice in implementing the Act (section 7(2)).

The use of electronic transactions is voluntary (section 8) unless mandated otherwise in another Act.

**Part 2** of the Act deals with the general principles underlying electronic transactions.

The Act is based on three fundamental principles underpinning those UNCITRAL texts: non-discrimination of electronic means; technology neutrality and functional equivalence. Those principles enable the use of electronic means by removing obstacles found in existing law, for instance with respect to form requirements assuming the use of the paper medium, and by adapting pre-existing legal notions to an online environment.

The principle of non-discrimination ensures that an electronic record is not denied legal effect, validity or enforceability solely on the grounds that it is in electronic form (sections 9, 11(1), 17(2)).

The principle of technology neutrality ensures that the law does not mandate or favour the use of any specific technology, method, product or model, thus allowing advancements in technology to be accommodated without the need for legislative change (implemented throughout the Act; stated explicitly in section 22 with respect to electronic signatures).

The principle of functional equivalence lays out criteria by which a data message is deemed to satisfy form requirements applicable to paper-based documents, such as the requirement that a document be in writing, in original form or signed (sections 10, 12, 23, 27).

It has to be noted that UNCITRAL provisions on functional equivalence refer to a requirement contained in "a rule of law". However, the reference to "rule of law" was replaced to a reference to "written law" at the request of OAG. It is understood that this is done in order to follow the customary Kiribati legal drafting style, and on the assumption that common law does not contain the requirements while statutory law (i.e., "written law") does. The amendment does not intend in any manner to limit the operation of functional equivalence rules regardless of the legal source of the form requirement.

**Part 3** of the Act deals with electronic contracting. In line with the UNCITRAL approach, it does not amend in any manner existing contract law but only enables the use of electronic means.

Besides adopting the above-mentioned general principles to electronic contracting, it clarifies that contractual statements on websites and a similar amount to an invitation to make an offer (and not to an offer) (section 18), and validates the use of automated agents to conclude contracts ("smart contracts") (sections 16(b) and 19). It also contains a rule safeguarding physical persons from the consequences of input errors (section 21).

**Part 4** of the Act deals with electronic signatures. Electronic signatures are a trusted service that offers assurance on the origin and integrity of an electronic communication.

The part contains two provisions: section 22 applies the principle of technology neutrality and section 23 the principle of functional equivalence.

Under section 23, all electronic communications that may be traced to an author may be considered signed (or not) according to circumstances. Those electronic signatures include: a telephone number linked to an SMS; the name typed in an email or the header of the email; a PKI certificate linked to an email, etc.

In case of dispute the judge will have to assess the various methods that may be used for electronic signatures, which have varying levels of reliability, in light of all circumstances including contractual agreements.

Section 22(3) acknowledges the current practice, e.g. in place at the Ministry of Fisheries, to purchase and use foreign PKI certificates to comply with international standards. Hence, all electronic signatures may be used in Kiribati, irrespective of geographic origin or place of use, and based only on their reliability. It is also not foreseen that local commercial providers of electronic signatures services will be available in the near future.

**Part 5** of the Act deals with electronic transferable records. Electronic transferable records are electronic records that incorporate the right to demand the payment of a sum of money or the delivery of goods. These are the electronic equivalents of commercial documents such as bills of lading, promissory notes and cheques.

This part enacts the UNCITRAL Model Law on Electronic Transferable Records (MLETR). The MLETR has been recently enacted in Singapore. Australia and New Zealand are expected to consider its adoption under the Digital Economy Agreements concluded with Singapore. It was therefore included in the Electronic Transactions Act to make it future proof with respect to smart logistics and paperless trade facilitation.

**Part 6** of the Act deals with electronic transactions with public bodies. As mentioned above, e-Government matters fall under the competence of the Ministry responsible for Communication and Information.

The Act is not applicable to transactions with public bodies unless regulations have been adopted.

It is understood that different ministries have varying levels of readiness to embrace digitalisation, and that therefore e-Government will be phased in gradually but in a coherent manner. Hence, the effect of the Act (section 35) is only to set out the general principles upon which the regulations will be built, so as to ensure interoperability.

**Part 7** of the Act deals with miscellaneous matters.

**Section 36** provides guidance on electronic evidence besides already given in section 11. These rules apply only to civil proceedings and do not displace the special rules for criminal proceedings. They also do not displace the rules already contained in the Evidence Act.

**Section 37** gives the authority to make regulations to the relevant Minister. It should be noted that the Act is self-executing and does not need any regulation to enter into force and apply to electronic transactions exchanged among traders, between traders and consumers and in other instances not involving public bodies.

#### **Reference materials**

As mentioned above, the Electronic Transactions Act substantive provisions are taken from the UNCITRAL Model Law on Electronic Commerce (MLEC), the United Nations Convention on the Use of Electronic Communications in International Contracts (ECC) and the UNCITRAL Model Law on Electronic Transferable Records (MLETR).

Detailed information on UNCITRAL texts is available on the UNCITRAL website at <https://uncitral.un.org/en/texts/ecommerce>. Such information includes explanatory notes for each UNCITRAL provision referenced in the Electronic Transactions Act.

The UNCITRAL website offers also information on case law applying UNCITRAL texts through the Case Law on UNCITRAL Texts (CLOUT) system at [https://uncitral.un.org/en/case\\_law](https://uncitral.un.org/en/case_law). Several of the cases law applying UNCITRAL texts on e-commerce originate from common law jurisdictions such as Australia, New Zealand and Singapore.

The following table provides the cross-reference between the provisions of the Act and the source UNCITRAL text. With that information, it is possible to easily obtain an in-depth explanation of each article of the Act by accessing the explanatory materials freely available on the UNCITRAL website.

Section of the Act	UNCITRAL reference	Section of the Act	UNCITRAL reference
<b>Part 1 - Preliminary</b>		<b>Part 4 - Electronic Signatures</b>	
1. Short title	n/a	22. Equal treatment of signature technologies	Art. 3 MLES
2. Commencement	n/a	23. Legal requirement for a signature	Art. 9(3) ECC; Art. 12 MLES
3. Definitions	Art. 2 MLEC; Art. 4 ECC; Art. 2 MLETR	<b>Part 5 - Electronic Transferable Records</b>	
4. Objective of the Act	n/a	24. Application of this Part	Art. 1 MLETR
5. Administration of the Act	n/a	25. Additional information in electronic transferable records	Art. 6 MLETR
6. Republic to be bound	n/a	26. General reliability standard	Art. 12 MLETR
7. Exclusions and General Power of Minister to exclude and include matters under Act	n/a	27. Legal requirement for an electronic transferable record	Art. 10 MLETR
8. Voluntary use of computer data	Art. 8(2) ECC	28. Control	Art. 11 MLETR
<b>Part 2 - Legal Recognition of Electronic Communications</b>		29. Indication of time and place in electronic transferable record	Art. 13 MLETR
9. Legal recognition of computer data and electronic communications	Art. 5 MLEC; Art. 5 bis MLEC	30. Endorsement	Art. 15 MLETR
10. Writing	Art. 6 MLEC	31. Amendment	Art. 16 MLETR

11. Admissibility and evidential weight of computer data and electronic communications	Art. 9 MLEC	32. Replacement of a transferable document or instrument with an electronic transferable record	Art. 17 MLETR
12. Legal requirement to retain information	Art. 8 MLEC	33. Replacement of an electronic transferable record with a transferable document or instrument	Art. 18 MLETR
13. Producing and retaining electronic versions of paper-based documents or records	n/a	34. Non-discrimination of foreign electronic transferable records	Art. 19 MLETR
14. Time and place of dispatch and receipt of electronic communications	Art. 10 ECC	<b>Part 6 - Electronic Exchanges with Public Bodies</b>	
15. Determining the place of business	Art. 6 ECC	35. Authorization for public bodies to use computer data and electronic signatures	n/a
<b>Part 3 - Electronic Contracting</b>		<b>Part 7- Miscellaneous</b>	
16. Attribution of electronic communications	Art. 13 MLEC	36. Rules governing electronic evidence	n/a
17. Formation and validity of contracts	Art. 11 MLEC	37. Powers to make Regulations	n/a
18. Invitations to make offers	Art. 11 ECC		
19. Use of automated message systems for contract formation	Art. 12 ECC		
20. Availability of contract terms	Art. 13 ECC		
21. Error in electronic communications	Art. 14 ECC		

**HONOURABLE BOOTINAUAN**  
**Minister for Commerce, Industry and Cooperatives**

**LEGAL REPORT**

I hereby certify that none of the provisions of the above Act conflict with the Constitution and that His Excellency the Beretitenti may properly assent to the Act.

**TETIRO MAATE SEMILOTA**  
**ATTORNEY GENERAL**

**CERTIFICATE OF THE CLERK OF THE MANEABA NI  
MAUNGATABU**

This printed impression of the Electronic Transactions Act 2021 has been carefully examined by me with the Bill which passed the Maneaba ni Maungatabu on the 11<sup>th</sup> August 2021 and is found by me to be a true and correctly printed copy of the said Bill.



**Eni Tekanene**  
**Clerk of the Maneaba ni Maungatabu**

Published by exhibition at the Maneaba ni Maungatabu this 21 day  
of September 2021.



**Eni Tekanene**  
**Clerk of the Maneaba ni Maungatabu**