

No. 38 of 2021.

Electronic Transactions Act 2021.

Certified on : 23 FEB 2022



No. 38 of 2021.

Electronic Transactions Act 2021.

ARRANGEMENT OF SECTIONS.

PART I. - PRELIMINARY.

1. Compliance with constitutional requirements.
2. Purpose of the Act.
3. Interpretation -
 - “addressee”
 - “automated message system”
 - “certificate”
 - “commercial”
 - “communication”
 - “data”
 - “data message”
 - “electronic address”
 - “electronic record”
 - “electronic signature”
 - “electronic system”
 - “electronic transferable record”
 - “intermediary”
 - “non-commercial”
 - “originator”
 - “party”
 - “place of business”
 - “quality of data”
 - “relying party”
 - “signatory”
 - “transaction”
 - “transferable document or instrument”
 - “trust service”
 - “trust service provider”.
4. Application.
5. Exclusions.

PART II. - ELECTRONIC TRANSACTIONS.

6. Party autonomy.
7. Location of the parties.
8. Information requirements.

9. Legal recognition of electronic records.
10. Requirement for writing.
11. Original form.
12. Admissibility and evidential weight of electronic records or data messages.
13. Retention of electronic records or data messages.
14. Recognition by parties of data messages.
15. Attribution of data messages.
16. Time and place of dispatch and receipt of data messages.
17. Acknowledgement of receipt.

PART III. - ELECTRONIC CONTRACTING.

18. Formation and validity of contracts.
19. Invitation to make offers.
20. Use of automated message systems for contract formation.
21. Availability of contract terms.
22. Error in data messages.
23. Additional information.

PART IV. - ELECTRONIC SIGNATURES AND TRUST SERVICES.

24. Equal treatment of signature technologies.
25. Electronic signatures.
26. Trustworthiness.
27. Recognition of foreign electronic signatures and trust services.
28. Conduct of the signatory.
29. Conduct of the trust service provider.
30. Conduct of the relying party.

PART V. - ELECTRONIC TRANSFERABLE RECORDS.

31. Electronic transferable records.
32. Legal recognition of an electronic transferable record.
33. Transferable documents or instruments.
34. Non-discrimination of foreign electronic transferable records.
35. Concept of control.
36. General reliability standard.
37. Indication of time and place in electronic transferable records.
38. Endorsement.
39. Amendment of a transferable document or instrument.
40. Replacement of a transferable document or instrument with an electronic transferable record.
41. Replacement of an electronic transferable record with a transferable document or instrument.

PART VI. - MISCELLANEOUS.

42. Regulations.



No. 38 of 2021.

AN ACT

entitled

Electronic Transactions Act 2021,

Being an Act to establish a legal framework for the use of electronic transactions for commercial and non-commercial purposes,

MADE by the National Parliament to come into operation in accordance with a notice in the National Gazette by the Head of State, acting with, and in accordance with, the advice of the Minister.

PART I. - PRELIMINARY.

1. COMPLIANCE WITH CONSTITUTIONAL REQUIREMENTS.

(1) For the purposes of Section 41 of the *Organic Law on Provincial Governments and Local-level Governments*, it is declared that this law relates to a matter of national interest.

(2) This Act, to the extent that it regulates or restricts a right or freedom referred to in Subdivision III.3.C. (*qualified rights*) of the *Constitution*, namely -

- (a) the right to freedom from arbitrary search and entry conferred by Section 44; and
- (b) the right to freedom of expression conferred by Section 46; and
- (c) the right to privacy conferred by Section 49; and
- (d) the right to freedom of information conferred by Section 51; and
- (e) the right to freedom of movement conferred by Section 52; and
- (f) the right to protection from unjust deprivation of property conferred by Section 53,

of the *Constitution*, that is necessary for the purpose of giving effect to the public interest in public order and public welfare and the development of under-privileged or less advanced groups or areas and is reasonably justifiable in a democratic society having proper respect and regard for the rights and dignity of mankind taking into account the National Goals and Directive Principles and Basic Social Obligations, in particular to the successful social and economic development of Papua New Guinea and its citizens.

2. PURPOSE OF THE ACT.

(1) The purpose of this Act is to establish the legal framework for the use of electronic transactions -

- (a) to facilitate electronic communications by means of reliable electronic records; and
- (b) to -
 - (i) facilitate electronic commerce; and
 - (ii) eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements; and
 - (iii) promote the development of the legal and business infrastructure necessary to implement secured electronic commerce; and

Electronic Transactions

- (c) facilitate electronic filing of documents with public agencies and to support the promotion of efficient delivery by public agencies of services by means of reliable electronic records; and
- (d) apply principles relevant to electronic transactions to minimise the incidence forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions; and
- (e) establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records; and
- (f) promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic form.

3. INTERPRETATION.

(1) In this Act, unless the contrary intention appears -

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

“automated message system” means a computer program or an electronic or other automated means used -

- (a) to initiate an action; or
- (b) to 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;

“certificate” means -

- (a) a data message; or
- (b) other record confirming the link between a signatory and signature creation data; or
- (c) the link between a trust service and its relevant trust service data;

“commercial” means relating to or connected with trade or commerce in general;

“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;

“data” includes -

- (a) any representation of facts; or
- (b) concepts; or
- (c) information (text, audio, video or images); or
- (d) machine readable code or instruction,

in a -

- (e) form suitable for processing in an electronic system; or
- (f) program suitable to cause an electronic system to perform a function;

“data message” means information generated, sent, received or stored by guided or unguided electronic, magnetic, optical or similar means, including, but not limited to, electronic data interchange, electronic communication, electronic mail, telegram, telex or telecopy;

“electronic address” means any number or address used for the purposes of sending or receiving data messages, electronic records, electronic communications, documents or information by electronic means and includes an e-mail address;

Electronic Transactions

“electronic record” means -

- (a) information generated, communicated, received or stored by electronic means; or
- (b) where appropriate, all information logically associated with or otherwise linked together so as to become part of the record, whether generated contemporaneously or not; or
- (c) a display printout or other output of those data such as audio, video or audio-visual recording or photographic images and may or may not have a paper record to prove the electronic record;

“electronic signature” means any symbol or other data in electronic form, 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;

“electronic system” means -

- (a) a system consisting of hardware or software; or
- (b) a group of interconnected or related systems or devices, one of which, under a program, performs automatic processing, generating, sending, receiving or storing of data, including but not limited to electronic devices, the internet input, output and storage facilities;

“electronic transferable record” is an electronic record that complies with the requirements under Section 33;

“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 in respect to that data message;

“non-commercial” refers to any activity or entity that does not involve commerce or trade;

“originator” of a data message means a person 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 person acting as an intermediary with respect to that data message;

“party” means any person involved in a transaction or proceeding;

“place of business” means -

- (a) any place where an individual or 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; or
- (b) in relation to government, an authority of government or a non-profit body - a place where any operations or activities are carried out by that government, authority or body;

“quality of data” means the qualitative or quantitative fitness of information for its intended use;

“relying party” means a person that may act on the basis of an electronic signature;

“signatory” means a person who holds signature creation data and acts on his own behalf or on behalf of the person he represents;

“transaction” means -

- (a) any dealings in the nature of a contract, agreement or other arrangement; or
- (b) 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 in connection with the formation or performance of a contract, agreement, or other arrangement; or
- (c) any transaction of a non-commercial nature;

Electronic Transactions

“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;

“trust service” means an electronic service that provides a certain level of reliability in the quality of data and includes electronic signatures, seals, time-stamps, delivery services and website authentication, any related certificate and their retention;

“trust service provider” means a person who provides services related to a trust service;

(2) In the interpretation of this Act, regard is to be made to its international origin to promote harmonisation and uniformity in its application and to observe good faith.

(3) Where there is no specific provision in this Act which deals with any legal issues that may arise, the issues shall be dealt with in accordance with -

- (a) the international law principles; and
- (b) general principles of civil and commercial practice; and
- (c) other laws and customary laws,

applicable in this country.

4. APPLICATION.

(1) This Act applies to any kind of data message and electronic record, electronic communication and electronic document used in the context of commercial and non-commercial activities including domestic and international -

- (a) dealings; and
- (b) transactions; and
- (c) arrangements; and
- (d) agreements; and
- (e) exchanges; and
- (f) storage of information.

(2) This Act is to be read in conjunction with and not in derogation of the provisions of the *Independent Consumer and Competition Commission Act 2002*.

5. EXCLUSIONS.

This Act does not apply to -

- (a) transactions on a regulated exchange; and
- (b) foreign exchange transactions; and
- (c) inter-bank payment systems, inter-bank payment agreements or clearance and settlement systems relating to securities or other financial assets or instruments; and
- (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; and
- (e) transactions and matters relating to private law including marriages, divorce, the creation or execution of a will or any other testamentary disposition; and
- (f) a Power-of-Attorney; and
- (g) a trust, excluding a constructive, implied and resulting trust; and
- (h) any documents (including affidavits, statutory declarations, or other documents involving an oath or affirmation) required to be attested before a notary public; and

Electronic Transactions

- (i) any other documents or transactions exempted by other laws in Papua New Guinea.

PART II. - ELECTRONIC TRANSACTIONS.

6. PARTY AUTONOMY.

(1) Nothing in this Act requires a party to use or accept electronic records, however, a party's agreement to use electronic records may be inferred from the party's conduct.

- (2) The effect of this Act may be -
 - (a) derogated from the party's agreement; or
 - (b) varied by agreement,

unless that agreement would not be valid or effective under any applicable law.

7. 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) Where a party who has more than one place of business and has not indicated a place of business, the place of business for the purposes of this Act is that which has the closest relationship to the underlying transaction.

- (3) Where a party location is to be determined, regard must be made to -
 - (a) the circumstances known to or contemplated by the parties at any time before or at the time of carrying out that transaction; or
 - (b) the principal place of business, where there is no underlying transaction.

(4) Where a person does not have a place of business, reference is to be made to the person's habitual residence.

- (5) A location is not a place of business merely because it is -
 - (a) where equipment and technology supporting an electronic system used by a party in connection with the formation of a contract is located; or
 - (b) where the electronic system may be accessed by other parties.

(6) Where a party makes use of a domain name or electronic mail address connected to a specific country, it does not create a presumption that its place of business is located in that country.

8. INFORMATION REQUIREMENTS.

Nothing in this Act affects the application of any law that may require the parties to disclose their identities, places of business or other information or data, or relieves a party from the legal consequences of making inaccurate, incomplete or false statements in that regard.

9. LEGAL RECOGNITION OF ELECTRONIC RECORDS.

(1) An information shall not be denied legal effect, validity or enforceability solely on the grounds that -

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

Electronic Transactions

- (b) the information is not contained in the data message that gives rise to such legal effect, but is merely referred to in that data message.

(2) Any information referred to in the data message shall be accessible to the person against whom the referred information is to be used.

10. REQUIREMENT FOR WRITING.

(1) Where the law requires information to be in writing and provides consequences if it is not, that requirement is met by a data message if the information contained in it is accessible so as to be usable for subsequent reference.

(2) Section 10(1) applies whether the requirement is in the form of an obligation or whether the law provides consequences for the information not being in writing.

11. ORIGINAL FORM.

(1) Where the law requires information to be presented or retained in its original form, the requirement is met by an electronic record or 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 -

- (a) the requirement of the information is in the form of an obligation; or
- (b) the law provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of Subsection (1)(a) -

- (a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered apart from the addition of any endorsement and change which in the normal course of communication, storage and display; and
- (b) the standard of reliability required shall be assessed taking into consideration the purpose for which the information was generated and taking into account all the relevant circumstances.

12. ADMISSIBILITY AND EVIDENTIAL WEIGHT OF ELECTRONIC RECORDS OR DATA MESSAGES.

The evidential requirements of admissibility and evidential weight of electronic records or data messages provided by the *Evidence Act* (Chapter 48) shall apply.

13. RETENTION OF ELECTRONIC RECORDS OR DATA MESSAGES.

(1) Where the law requires that certain documents, records or information are to be retained, that requirement is met by retaining electronic records or data messages in accordance with Subsection 2.

(2) The retention of certain documents, records or information in Subsection (1) is made if -

- (a) the information contained in the electronic records or data messages is accessible to be usable for subsequent reference; and

Electronic Transactions

- (b) the electronic record or data message is retained -
 - (i) in the format in which it was generated, sent or received; or
 - (ii) in a format which can be demonstrated to represent accurately the information generated, sent or received; and
- (c) such information, if any, is retained to enable the identification of the origin and destination of an electronic record or data message and the date and time when it was sent or received.

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

(4) A person may satisfy the requirement referred to in Subsection (1) by using the services of any other person, if the conditions provided under Subsections (1) and (2) are met.

14. RECOGNITION BY PARTIES OF DATA MESSAGES.

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

15. ATTRIBUTION OF DATA MESSAGES.

(1) A data message is that of the originator, if the data message was sent by -

- (a) the originator himself or itself; or
- (b) a person who has the authority to act on behalf of the originator in respect of that data message; or
- (c) an electronic system programmed by, or on behalf of the originator to operate automatically.

(2) The addressee is entitled to assume that a data message is that of the originator and to act upon that assumption, if -

- (a) in order to ascertain whether the data message is that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or
- (b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(3) Subsection (2) does not apply -

- (a) as of the time when -
 - (i) the addressee has received notice from the originator that the data message is not that of the originator; and
 - (ii) the addressee had reasonable time to act accordingly; or
- (b) in a case with Subsection (2)(b), at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure that the data message was not that of the originator.

(4) Where -

- (a) a data message is that of the originator; or
- (b) a data message is deemed to be that of the originator; or

Electronic Transactions

(c) the addressee is entitled to act on the assumption that a data message is that of the originator,
the addressee is entitled to regard the data message received as being what the originator intended to send, and to act on that assumption.

(5) The addressee is not entitled to regard the data message received as being what the originator intended to send and to act on that assumption, when it knew or should have known, had the addressee exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption.

(7) Subsection (6) does not apply if the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

16. TIME AND PLACE OF DISPATCH AND RECEIPT OF DATA MESSAGES.

(1) Unless otherwise agreed between the originator and the addressee, the time of dispatch of a data message is the time when it leaves an information electronic system under the control of the originator or of the party who sends it on behalf of the originator.

(2) If the data message has not left immediately (at any time interval) an information system under the control of the originator or of the party who sends it on behalf of the originator, the reference should be to the time when the data message is received.

(3) Unless otherwise agreed between the originator and the addressee, 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.

(4) 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.

(5) A data message is presumed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

(6) 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 7.

(7) Subsection (6) applies notwithstanding that the place where the electronic system supporting an electronic address is located may be different from the place where the data message is deemed to be received.

17. ACKNOWLEDGEMENT OF RECEIPT.

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

Electronic Transactions

(2) Where the originator has not agreed with the addressee that the acknowledgement is to be given in a particular form or by a particular method, an acknowledgment 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 by the originator.

(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), the originator 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.

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

(7) Except as 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.

(8) Presumption under Subsection (5) does not imply that the data message corresponds to the message received.

PART III. - ELECTRONIC CONTRACTING.

18. FORMATION AND VALIDITY OF CONTRACTS.

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

(2) Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

19. INVITATION TO MAKE OFFERS.

(1) A proposal to conclude a contract may be made through one or more data messages.

(2) The proposal is not addressed to one or more specific parties, but is generally accessible to parties making use of electronic systems.

Electronic Transactions

(3) The proposal in Subsection (1) includes proposals that make use of interactive applications for the placement of orders through the electronic systems and is considered as an invitation to make offers unless it clearly indicates that the intention of the party making the proposal is to be bound in case of acceptance.

20. USE OF AUTOMATED MESSAGE SYSTEMS FOR CONTRACT FORMATION.

A contract formed by the interaction of an automated message system and a 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.

21. AVAILABILITY OF CONTRACT TERMS.

Nothing in this Act affects the application of any other law that may require a party who negotiates some or all of the terms of a contract through the exchange of electronic communications to make available to the other party those data messages which contain the contractual terms in a particular manner, or relieves a party from the legal consequences of its failure to do so.

22. ERROR IN DATA MESSAGES.

(1) Where a natural person makes an input error in a data message 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.

(2) Subsection (1) applies 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 made an error in the data message; 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.

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

23. ADDITIONAL INFORMATION.

Nothing in this Act precludes the inclusion of information -

- (a) in an electronic record; or
- (b) in a data message; or
- (c) in an electronic transferable record in addition to that contained in a paper-based document; or
- (d) in a transferable document or instrument.

PART IV. - ELECTRONIC SIGNATURES AND TRUST SERVICES.

24. EQUAL TREATMENT OF SIGNATURE TECHNOLOGIES.

Nothing in this Act must be applied, unless upon the principle of party autonomy as described in Section 6 to exclude, restrict or deprive of legal effect any method of creating an electronic signature that -

- (a) satisfies the requirements referred to in Section 25; or
- (b) otherwise meets the requirements under other applicable laws.

Electronic Transactions

25. ELECTRONIC SIGNATURES.

(1) Subject to Subsection (2) where the law requires the signature of a person or a party in relation to electronic record or data message, that requirement of the law is satisfied if an electronic signature is used.

(2) The electronic signature is as reliable as was appropriate for the purpose for which the electronic record or data message was generated or communicated, taking into consideration all the circumstances, including any relevant agreement.

(3) Subsection (1) applies whether -

- (a) the requirement referred to in Subsection (1) is in the form of an obligation; or
- (b) the law provides consequences for the absence of a signature.

(4) An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in Subsection (1) if -

- (a) the signature creation data is within the context in which it is used, linked to the signatory and of no other person or party; and
- (b) the signature creation data was, at the time of signing, under the control of the signatory and of no other person or party; and
- (c) any alteration to the electronic signature, made after the time of signing, is detectable; and
- (d) the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

(5) Subsection (4) does not limit the ability of any person or party -

- (a) to establish, in any other way, for the purpose of satisfying the requirement referred to in Subsection (1), the reliability of an electronic signature; or
- (b) to adduce evidence of the non-reliability of an electronic signature.

26. TRUSTWORTHINESS.

For the purposes of Section 29(1)(g), in determining whether or to what extent, any systems, procedures and human resources utilised by a trust service provider are trustworthy, regard may be given to the following factors:

- (a) financial and human resources, including existence of assets; and
- (b) quality of hardware and software systems; and
- (c) procedures for processing electronic signatures and applications for electronic signatures and retention of records; and
- (d) availability of information to signatories identified in electronic signatures and to potential relying parties; and
- (e) regularity and extent of audit by an independent body; and
- (f) the existence of a declaration by an accreditation body or the service provider regarding compliance with or existence of the factors in Paragraphs (a), (b), (c), (d) and (e); and
- (g) any other relevant factors.

27. RECOGNITION OF FOREIGN ELECTRONIC SIGNATURES AND TRUST SERVICES.

(1) In determining whether, or to what extent, a trust service, or an electronic signature, is legally effective, there shall not be any consideration -

- (a) to the geographic location where the trust service is issued or the electronic signature is created or used; or

Electronic Transactions

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

(2) A trust service issued or an electronic signature created or used outside Papua New Guinea shall have the same legal effect in Papua New Guinea as a trust service issued or an electronic signature created or used within Papua New Guinea if it offers a substantially equivalent level of reliability.

(3) For purposes of Subsection (2), to determine whether a trust service or an electronic signature offers a substantially equivalent level of reliability, regard must be given to recognise international standards and to any other relevant factors.

(4) Notwithstanding Subsections (2) and (3), where parties agree to the use of certain types of electronic signatures, that agreement must be recognised as sufficient for the purposes of cross-border recognition, unless that agreement would be valid or effective under other applicable laws.

28. CONDUCT OF THE SIGNATORY.

(1) Where a signature creation data is used to create a signature that has legal effect, each signatory shall -

- (a) exercise reasonable care to avoid unauthorised use of its signature creation data; and
 - (b) without undue delay -
 - (i) utilise means made available by the service provider pursuant to Section 29(1)(d)(v); or
 - (ii) otherwise use reasonable efforts to notify any person or party that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature,
- if -
- (iii) the signatory knows that the signature creation data have been compromised; or
 - (iv) the circumstances known to the signatory give rise to a substantial risk that the signature creation data may have been compromised.

(2) Where a certificate is used to support the electronic signature, the signatory shall exercise reasonable care to ensure the accuracy and completeness of all material representations are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

(3) A signatory shall bear the legal consequences of its failure to satisfy the requirements of Subsection (1).

29. CONDUCT OF THE TRUST SERVICE PROVIDER.

(1) Where a trust service provider provides services to support an electronic signature that may be used for legal effect as a signature, that service provider shall -

- (a) act in accordance with representations made by it with respect to its policies and practices; and
- (b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the trust service throughout its life cycle or that are included in the trust service; and
- (c) provide reasonably accessible means that enable a relying party to ascertain from the electronic trust service -
 - (i) the identity of the trust service provider; and
 - (ii) that the signatory that is identified in the trust service has control of the signature creation data at the time when the electronic signature is issued; and

Electronic Transactions

- (iii) that signature creation data was valid at or before the time when the trust service was issued; and
- (d) provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the trust service or otherwise -
 - (i) the method used to identify the signatory; and
 - (ii) any limitation on the purpose or value for which the signature creation data or the trust service may be used; and
 - (iii) that the signature creation data is valid and has not been compromised; and
 - (iv) any limitation on the scope or extent of liability stipulated by the trust service provider; and
 - (v) whether means exist for the signatory to give notice pursuant to Section 27(1)(b); and
 - (vi) whether a timely revocation service is offered; and
- (e) for purposes of Subsection (1)(d)(v), provide a means for a signatory to give notice pursuant to Section 27(1)(b); and
- (f) for purposes of Subsection (1)(d)(vi), ensure the availability of a timely revocation service; and
- (g) utilise trustworthy systems, procedures and human resources in performing its services.

(2) A trust service provider shall bear the legal consequences of its failure to satisfy the requirements under Subsection (1).

30. CONDUCT OF THE RELYING PARTY.

A relying party shall bear the legal consequences of its failure -

- (a) to take reasonable steps to verify the reliability of a trust service; or
- (b) where an electronic signature is supported by a certificate, to take reasonable steps -
 - (i) to verify the validity, suspension or revocation of the certificate; and
 - (ii) to observe any limitation with respect to the certificate.

PART V. - ELECTRONIC TRANSFERABLE RECORDS.

31. ELECTRONIC TRANSFERABLE RECORDS.

(1) Nothing in this Act affects the application to an electronic transferable record of any other law governing a transferable document or instrument including any other law applicable to consumer protection.

(2) This part does not apply to the documents excluded under Section 5 including securities and other investment instruments.

32. LEGAL RECOGNITION OF AN ELECTRONIC TRANSFERABLE RECORD.

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

(2) Nothing in this Act requires a person to use an electronic transferable record without that person's consent.

(3) The consent of a person to use an electronic transferable record may be inferred from the person's conduct.

Electronic Transactions

(4) The parties are bound by any obligation that arises from the electronic transferable record.

33. TRANSFERABLE DOCUMENTS OR INSTRUMENTS.

(1) Where the law requires a transferable document or instrument, that requirement is met by an electronic record if -

- (a) the electronic record 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 electronic record as the electronic transferable record; and
 - (ii) to render that electronic record 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 electronic record.

(2) The criterion for assessing integrity under Subsection (1)(b)(iii) shall be -

- (a) whether the data or information contained in the electronic transferable record; and
- (b) any authorised change that arises from its creation until it ceases to have any effect or validity,

have remained complete and unaltered apart from any change which arise in the normal course of communication, storage and display.

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 outside of Papua New Guinea.

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

35. CONCEPT OF 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 the 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.

36. GENERAL RELIABILITY STANDARD.

For the purposes of Sections 33(1)(b), 35(1), 37, 39, 40(1) and 41(1), the method referred to shall be -

- (a) as reliable as appropriate to fulfill the function for which the method is being used, taking into account all relevant circumstances, which may include -
 - (i) any operational rules relevant to the assessment of reliability; or
 - (ii) the assurance of data integrity; or
 - (iii) the ability to prevent unauthorised access to and use of the system; or
 - (iv) the security of hardware and software; or
 - (v) the regularity and extent of audit by an independent body; or
 - (vi) the existence of a declaration by a supervisory body, an accreditation body or a voluntary scheme regarding the reliability of the method; or

Electronic Transactions

- (vii) any applicable industry standard; and
- (b) proven to have fulfilled the function by itself or together with further evidence.

37. 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.

38. ENDORSEMENT.

Where the law requires the endorsement in any form of a transferable document or instrument, that requirement is met with respect to an electronic transferable record if -

- (a) the information required for the endorsement is included in the electronic transferable record; and
- (b) that information is compliant with the requirements under Sections 10 and 25 in relation to writing and electronic signatures.

39. AMENDMENT OF A TRANSFERABLE DOCUMENT OR INSTRUMENT.

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.

40. 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 form is used.

(2) For the change of form to take effect, a statement indicating a change of form must 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 form in accordance with Subsections (1) and (2) shall not affect the rights and obligations of the parties.

41. 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 form is used.

(2) For the change of form to take effect, a statement indicating a change of form must 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 must be made inoperative and ceases to have any effect or validity.

(4) A change of form in accordance with Subsections (1) and (2) must not affect the rights and obligations of the parties.

Electronic Transactions

PART VI. - MISCELLANEOUS.

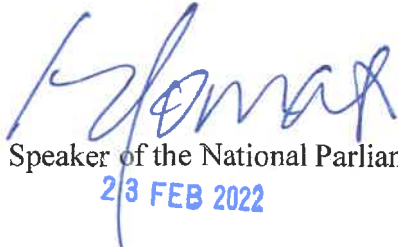
42. REGULATIONS.

The Head of State, acting on advice, may make regulations, not inconsistent with this Act, prescribing all matters, required or permitted to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to this Act.

I hereby certify that the above is a fair print of the *Electronic Transactions Act 2021*, which has been made by the National Parliament.


Clerk of the National Parliament.
23 FEB 2022

I hereby certify that the *Electronic Transactions Act 2021*, was made by the National Parliament on 18 November 2021, by an absolute majority in accordance with the *Constitution*.


Speaker of the National Parliament.
23 FEB 2022