

No. of 2019

**VIRGIN ISLANDS**  
**ELECTRONIC TRANSACTIONS ACT, 2019**  
**ARRANGEMENT OF SECTIONS**

*Section*

**PART I**  
**PRELIMINARY**

1. Short title and commencement.
2. Interpretation.
3. Act binds the Crown.
4. Non-application.
5. Autonomy of parties.

**PART II**  
**REQUIREMENTS FOR LEGAL RECOGNITION**

6. Legal recognition of electronic communications.
7. Writing.
8. Furnishing information in prescribed form.
9. Access to information in paper form.
10. Delivery of information.
11. Information in original form.
12. Retention of documents, records, or information.
13. Other requirements.
14. Comparison of documents with originals.
15. Admissibility of electronic communications.

**PART III**  
**ELECTRONIC CONTRACTS**

16. Formation and validity of contracts.
17. Recognition of electronic communication between parties.
18. Time and place of dispatch and receipt of electronic communications.
19. Use of automated message systems for contract formation.
20. Error in electronic communications.

**PART IV**  
**SECURE ELECTRONIC SIGNATURES AND RECORDS**

21. Requirement for signature.
22. Equal treatment of signatures.
23. Conduct of the signatory.
24. Recognition of foreign certificates and electronic signatures.
25. Secure electronic record and secure electronic signature.
26. Presumptions related to secure electronic records and signatures.

**PART V**  
**INTERMEDIARIES AND ELECTRONIC COMMERCE SERVICE PROVIDERS**

27. Liability of intermediaries and electronic commerce service providers.
28. Procedure for dealing with unlawful, defamatory etc. information.
29. Codes of conduct and standards for intermediaries and electronic commerce service providers.

**PART VI**  
**MISCELLANEOUS**

30. Specified security procedure providers.
31. Information to be provided to consumers.
32. Unwanted communications.
33. False or misleading information.
34. Offences by bodies corporate.
35. Regulations.
36. Repeal and savings.

I Assent

Governor  
, 2019

**VIRGIN ISLANDS**

No. of 2019

**A Bill for**

**An Act** to provide for the facilitation and regulation of electronic communications and electronic transactions and for related matters.

[Gazetted , 2019]

ENACTED by the Legislature of the Virgin Islands as follows:

**PART I  
PRELIMINARY**

- 1.** (1) This Act may be cited as the Electronic Transactions Act, 2019. Short title and commencement.
- (2) This Act shall come into force on such date as the Minister may, by Notice published in the Gazette, appoint.
- 2.** (1) In this Act Interpretation.
- “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 person acting as an intermediary with respect to that electronic communication;
- “authentication data” includes user name, password and license key;

“automated message system” means a computer programme or an electronic or other automated means used to initiate an action, or respond to electronic communication 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 programme or other automated means;

“certificate” means an electronic record or other record which confirms the link between a signatory and the signature creation data;

"communication" includes any statement, declaration, demand, notice, request, offer or 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;

“consumer” means any person who enters or intends to enter into an electronic transaction with a supplier as the end user of the goods or services offered by the supplier;

“Court” means the High Court;

“electronic” means relating to technology having electrical, digital, magnetic, wireless, optical, electro-magnetic, biometric, photonic or similar capabilities and references to carrying out any act “electronically” shall be construed similarly;

“electronic commerce service provider” means a person who uses electronic means in providing goods or services, or both;

“electronic communication” means a communication by electronic means of electronic records;

“electronic record” means information that is generated, communicated, received, or stored by electronic means or in an electronic system for transmission from one information system to another and includes a display, print out or other output of that information;

“individual” means a natural person;

“information” includes data, text, documents, records, electronic records, images, sounds, codes, computer programmes, software and databases;

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

“intermediary”, with respect to an electronic communication, means a person including a host who on behalf of another person, sends, receives, or stores either temporarily or permanently that electronic communication or provides related services with respect to that electronic communication, and includes telecommunication service providers, network service providers, internet service providers, search engines, online payment sites, online auction sites, online marketplaces and cyber cafés;

“Minister” means the Minister to whom responsibility for E-Commerce is assigned;

“originator”, in relation to an electronic communication, means a person who sends, or on whose behalf, the electronic communication has been sent or generated prior to storage, if any, but does not include an intermediary;

“public authority” means any Ministry, department, agency, board, commission or other body of the Government and includes an entity or body established by or under an enactment, or set-up by the Government in the public interest with or without an Act of the Legislature of the Virgin Islands;

“record” means information that is recorded, stored or otherwise maintained on a tangible medium or that is stored in an electronic, paper-based or other medium and is retrievable in visible form;

“secure electronic record” means an electronic record that is treated as a secure electronic record by virtue of section 25 of this Act;

“secure electronic signature” means an electronic signature that is treated as a secure electronic signature by virtue of section 25 of this Act;

“security procedure” means a procedure established by law or agreement or knowingly adopted by each party, that is employed for the purpose of

- (a) verifying that an electronic signature, communication is that of a particular person; or
- (b) for detecting changes or errors in content of an electronic communication;

“security procedure provider” means a person involved in the provision of a security procedure, or is specified as a security procedure provider by virtue of section 30 of this Act ; and

“signatory” means a person who may or may not hold a signature creation device and acts either on his or her own behalf or on behalf of another person to create an electronic signature;

“signature creation data” means unique data, including codes or private cryptographic keys or a uniquely configured physical device which is used by the signatory in creating an electronic signature;

“signed” or “signature” and its grammatical variations means a method, electronic or otherwise, used to identify a person and to indicate the intention of that person in respect of the information contained in a record;

“transaction” means an action or set of actions relating to the conduct of business, consumer or commercial affairs between two or more persons including the sale, lease, exchange, licensing or other disposition of personal property, including goods and intangible interests in real property, services or any combination of any of these acts.

(2) In this Act, “place of business”, means

- (a) in relation to a person, any place where the person 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) if the person does not have a place of business, the person's habitual residence; and
  - (c) in relation to a public authority or other body, a place where operations or activities are carried out by that public authority or other body.
- (3) For the purposes of subsection (2)
- (a) if a person has indicated his or her place of business, the location indicated by the person is presumed to be his or her place of business unless another person proves that the person making the indication does not have a place of business at that location;
  - (b) if a person has not indicated a place of business and has more than one place of business, then the place of business is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract;
  - (c) a location is not a place of business merely because that location is
    - (i) where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or
    - (ii) where the information system may be accessed by other parties; and
  - (d) the sole fact that a person makes use of a domain name or an electronic mail address connected to a specific country does not create a presumption that person's place of business is located in the country.

(4) Where an electronic communication does not relate to any contract, references to a contract in subsection (3) shall refer to the relevant transaction.

**3.** This Act binds the Crown.

Act binds the Crown.

Non-application.

**4. (1)** This Act does not apply to any law requiring writing, signatures or original documents for

- (a) the making, execution, amendment or revocation of a will or testamentary instrument;
- (b) the conveyance of real or personal property or the transfer of any interest in real or personal property;
- (c) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney;
- (d) the production of documents relating to immigration, citizenship or passport matters;
- (e) any other thing required to be done by deed; or
- (f) any other matters that may be prescribed by the Minister by Order.

(2) Notwithstanding subsection (1), the Minister may by Order make this Act applicable to any of the legal requirements set out in subsection (1).

(3) An Order made under subsection (2) shall be subject to a negative resolution of the House of Assembly.

Autonomy of parties.

**5. (1)** Nothing in this Act shall

- (a) require any person to use or accept electronic communications, electronic signatures or electronic contracts; or
- (b) prohibit any person engaging in a transaction through the use of electronic means from
  - (i) varying by agreement any provision of Parts II, III, and IV; or

- (ii) establishing reasonable requirements about the manner in which electronic communications, electronic signatures or electronic forms of documents may be accepted.

(2) A transaction which has been conducted using electronic means shall not be denied legal effect or validity solely on the ground of the type or method of electronic communication, electronic signature or electronic authentication selected by the parties.

## **PART II REQUIREMENTS FOR LEGAL RECOGNITION**

**6.** Information shall not be denied legal effect or validity solely on the ground that it is

Legal recognition of electronic communications.

- (a) in the form of an electronic communication; or
- (b) not contained in the electronic communication purporting to give rise to such legal effect, but is referred to in that electronic communication.

**7. (1)** Where a law requires any information or other matter to be in writing or in printed form or is described as being written, such requirement or description is satisfied if the information or matter is

Writing.

- (a) given in the form of an electronic communication; and
- (b) accessible to, and is capable of retention by, the addressee for subsequent reference.

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

(3) Where subsection (1) applies, a legal requirement to provide multiple copies of any information or other matter to the same person at the same time is satisfied by providing a single electronic record of the information or other matter.

(4) Where any information is retained electronically in accordance with subsection (1) and is retrievable at any time during the specified period of

retention, the paper or other non-electronic form of that information need not be retained.

Furnishing  
information in  
prescribed forms.

**8.** Where a law requires a person to provide information in a prescribed paper or other non-electronic form to another person that requirement is satisfied by providing the information electronically

- (a) in a format that contains the same or substantially the same information as the prescribed paper or other non-electronic form;
- (b) so that it is accessible to the other person and is usable or retrievable for subsequent reference; and
- (c) so that it is capable of being retained by the other person.

Access to  
information in  
paper form.

**9.** Where a law requires a person to provide access to information that is in paper or other non-electronic form that requirement is satisfied by providing access to the information electronically where

- (a) the form and means of access to the information reliably assures the maintenance of the integrity of the information, given the purpose for which, and the circumstances in which, access to the information is required to be provided; and
- (b) the person to whom access is required to be provided, consents to accessing the information electronically.

Delivery of  
information.

**10. (1)** Where a law requires information to be delivered or sent to, or to be served on, a person, that requirement may be satisfied by doing so in the form of an electronic communication if the originator of the electronic communication states that the receipt of the electronic communication is to be acknowledged and the addressee has acknowledged its receipt.

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

Information in  
original form.

**11. (1)** Where the law requires information to be presented or retained in its original form, that requirement is satisfied by an electronic communication if

- (a) there exists a reliable assurance as to the integrity of the information from the time it was first generated in its final form as an electronic communication or otherwise; and
- (b) that information is capable of being accurately represented to the person to whom it is to be presented.

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

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

- (a) the criterion for assessing the integrity of the information is whether the information has remained complete and unaltered, apart from the additions of any endorsement or any change which arises in the normal course of communication, storage and display; and
- (b) the standard of reliability required is to be assessed in the light of the purpose for which the information was generated and all the relevant circumstances.

**12. (1)** Where a law requires any documents, records or information to be retained, that requirement is satisfied by retaining the documents, records or information electronically if the following conditions are satisfied:

Retention of documents, records or information.

- (a) the information is accessible so as to be usable for subsequent reference;
- (b) the information is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
- (c) the information identifies the origin and destination of the information and the date and time when it was sent or received, is retained.

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

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions set out in subsection (1) are satisfied.

(4) Nothing in this section shall preclude any public authority from specifying additional requirements for the retention of information electronically where that information is subject to the jurisdiction of that public authority.

Other requirements.

**13. (1)** An expression in a law, whether used as a noun or verb, including the terms “document”, “record”, “file”, “submit”, “lodge”, “deliver”, “issue”, “publish”, “write in”, “print” or words or expressions of similar effect, shall be interpreted so as to include or permit such form, format or action in relation to an electronic communication unless otherwise provided for in this Act.

(2) Where a seal is required by law to be affixed to a document and such law does not prescribe the method or form by which such document may be sealed electronically, that requirement is satisfied if the document indicates that it is required to be under seal and it includes the secure electronic signature of the person by whom it is required to be sealed.

(3) Where a law or agreement requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, the requirement is satisfied if, the electronic signature of the person authorised to perform those acts, together with all other information required to be included by any other applicable law, is attached to the electronic signature or electronic record.

Comparison of documents with original.

**14.** Where a law requires that a document be compared with an original, that requirement is satisfied by comparing that document with an electronic version of the original document if the electronic version reliably assures the maintenance of the integrity of the document.

Admissibility of electronic communications.

**15. (1)** In proceedings in a court, tribunal or arbitration, whether of a legal, judicial, quasi-judicial or administrative nature, the admissibility of an electronic record or an electronic signature in evidence shall not be denied solely on the grounds that it is in the form of an electronic communication.

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

- (a) the reliability of the manner in which the electronic communication was generated, stored or transmitted;
- (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 factor.

### **PART III ELECTRONIC CONTRACTS**

**16. (1)** Unless otherwise agreed by the parties, an offer or the acceptance of an offer, or any matter that is material to the formation or operation of a contract may be expressed by means of electronic communications.

Formation and validity of contracts.

(2) Where an electronic communication is used in the formation of a contract, that contract shall not be denied legal effect or validity solely on the ground that an electronic communication was used.

(3) A proposal to conclude a contract, made through one or more electronic communications, which is not addressed to one or more specific parties, but is generally accessible to parties making use of an information system, including a proposal that makes use of interactive applications for the placement of orders through such information system, is to be considered as an invitation to make offers, unless it clearly indicates the intention of the party making the proposal to be bound in case of acceptance.

**17.** As between the originator and the addressee of an electronic communication, a declaration of intent or other statement shall not be denied legal effect or validity solely on the ground that it is in the form of an electronic communication.

Recognition of electronic communication by parties.

Time and place of dispatch and receipt of electronic communications.

- 18.** (1) The time of dispatch of an electronic communication is
- (a) the time when the electronic communication leaves an information system under the control of the originator; or
  - (b) if the electronic communication has not left an information system under the control of the originator, the time when the electronic communication is received.

- (2) The time of receipt of an electronic communication
- (a) is the time when the electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee; or
  - (b) is the time when the electronic communication has been sent to an electronic address of the addressee that is not a designated address and the
    - (i) addressee becomes aware that the electronic communication has been sent to that address; and
    - (ii) the electronic communication becomes capable of being retrieved by the addressee at that address.

(3) For the purposes of subsection (2)(b), an electronic communication is presumed to be capable of being retrieved by the addressee when it reaches the electronic address of the addressee.

(4) 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.

(5) Subsections (2) and (3) shall apply notwithstanding that the place where the information system supporting an electronic address is located may be different from the place where the electronic communication is deemed to be received under subsection (4).

Use of automated message systems for contract formation.

**19.** 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 legal effect or validity solely on the ground that a person did not review or intervene in each of the actions carried out by the automated message

systems or the resulting contract.

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

Error in electronic communications.

(2) Subsection (1) shall 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 an error was made 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 shall affect the application of any rule of law that may govern the consequences of any error other than as provided for in subsections (1) and (2).

#### **PART IV SECURE ELECTRONIC SIGNATURES AND RECORDS**

**21.** (1) Where a law or agreement requires a signature, that requirement is satisfied in relation to an electronic communication if

Requirement for signature.

- (a) a method is used to identify the person and to indicate that the person intended to sign or otherwise adopt the information in the electronic communication; and
- (b) the method used is

- (i) as reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
- (ii) proven to have fulfilled the functions described in paragraph (a), by itself or together with further evidence.

(2) The Minister may prescribe methods for identifying persons for the purposes of subsection (1).

(3) Where an electronic signature is required by the parties to an electronic transaction and the parties have not agreed on the type of electronic signature to be used, the requirement is satisfied in relation to the electronic transaction if

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

(4) Subsection (3) does not limit the ability of a person

- (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.

Equal treatment  
of signatures.

**22.** (1) Unless otherwise provided by law, the parties to an electronic transaction may agree to the use of a particular method or form of electronic signature or security procedure.

**23.** Where signature creation data or authentication data can be used to create a signature or authenticate any electronic communication that has legal effect, each signatory shall Conduct of the signatory.

- (a) exercise reasonable care to avoid unauthorised use of his or her signature creation data or authentication data;
- (b) without undue delay, notify any person who may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if
  - (i) the signatory knows that the signature creation data or authentication data has been compromised; or
  - (ii) the circumstances known to the signatory give rise to a substantial risk that the signature creation data or authentication data may have been compromised; and
- (c) where a certificate is used to support the electronic signature or authentication data, exercise reasonable care to ensure the accuracy and completeness of all material representation made by the signatory, which are relevant to the certificate throughout its lifecycle, or which are to be included in the certificate.

**24. (1)** In determining whether, or the extent to which, a certificate or an electronic signature is legally effective, no regard shall be had to the place where the certificate or the electronic signature was issued, nor to the jurisdiction in which the issuer had its place of business. Recognition of foreign certificates and electronic signatures.

(2) Parties to commercial and other transactions may specify that a particular security procedure provider, class of security procedure providers or class of certificates shall be used in connection with electronic communication or signatures submitted to them.

(3) Where the parties to a transaction agree to the use of particular types of electronic signatures and certificates, that agreement shall be recognised as sufficient for the purpose of cross-border recognition in respect of that transaction.

Secure electronic record and secure electronic signature.

**25. (1)** If a security procedure, or a commercially reasonable security procedure agreed to by the parties involved, has been properly applied to an electronic record to verify that the electronic record has not been altered since a specific point in time, such record shall be treated as a secure electronic record from such specific point in time to the time of verification.

(2) If, through the application of a security procedure, or a commercially reasonable security procedure agreed to by the parties involved, it can be verified that an electronic signature was, at the time it was made

- (a) unique to the person using it;
- (b) capable of identifying such person;
- (c) created in a manner or using a means under the sole control of the person using it; and
- (d) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated,

such signature shall be treated as a secure electronic signature.

(3) For the purposes of this section, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including

- (a) the nature of the transaction;
- (b) the sophistication of the parties;
- (c) the volume of similar transactions engaged in by either or all parties;
- (d) the availability of alternatives offered to, but rejected by, any party;
- (e) the cost of alternative procedures; and
- (f) the procedures in general use for similar types of transactions.

**26. (1)** In any proceedings involving a secure electronic record, it shall be presumed, unless evidence to the contrary is adduced, that

Presumptions relating to secure electronic records and signatures.

- (a) the secure electronic record has not been altered since the specific point in time to which the secure status relates;
- (b) the secure electronic signature is the signature of the person to whom it correlates; and
- (c) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

(2) In the absence of a secure electronic record or a secure electronic signature, nothing in this section and section 25 shall create any presumption relating to the authenticity and integrity of the electronic record or electronic signature.

**PART V  
INTERMEDIARIES AND ELECTRONIC COMMERCE SERVICE  
PROVIDERS**

**27. (1)** An intermediary or electronic commerce service provider shall not be subject to any civil or criminal liability in respect of any information contained in an electronic record in respect of which the intermediary or electronic commerce service provider provides services, if the intermediary or electronic commerce service provider was not the originator of the record and

Liability of intermediaries and electronic commerce service providers.

- (a) has no actual knowledge that the information gives rise to civil or criminal liability;
- (b) is not aware of any facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known; or
- (c) follows the procedure set out in section 28 if the intermediary or electronic commerce service provider
  - (i) acquires knowledge that the information gives rise to criminal liability, or

- (ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

(2) An intermediary or electronic commerce service provider is not required to monitor any electronic communication processed by means of that provider's system in order to ascertain whether its processing would constitute or give rise to an offence or give rise to civil liability.

(3) Nothing in this section shall relieve an intermediary or electronic commerce service provider from

- (a) any obligation to comply with an order or direction of a court or other competent authority; or
- (b) any contractual obligation.

Procedure for dealing with unlawful, defamatory etc. information.

**28.** (1) If an intermediary or electronic commerce service provider has actual knowledge that the information in an electronic record gives rise to civil or criminal liability, as soon as practicable the intermediary or electronic commerce service provider shall

- (a) remove the information from any information system within the intermediary's or electronic commerce service provider's control and cease to provide or offer to provide services in respect of that information; and
- (b) notify the Minister and appropriate law enforcement agency of the relevant facts and of the identity of the person for whom the intermediary or electronic commerce service provider was supplying services in respect of the information, if the identity of that person is known to the intermediary or electronic commerce service provider.

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

- (a) follow the relevant procedure set out in any code of conduct approved or standard specified under this Act if such code or standard applies to the intermediary or electronic commerce service provider; or
- (b) notify the Minister.

(3) Where the Minister is notified in respect of any information under subsection (2), the Minister may direct the intermediary or electronic commerce service provider to

- (a) remove the electronic record from any information processing system within the control of the intermediary or electronic commerce service provider ;
- (b) cease to provide services to the person to whom the intermediary or electronic commerce service provider was supplying services in respect of that electronic record;
- (c) cease to provide services in respect of that electronic record.

(4) An intermediary or electronic commerce service provider is not liable, to any person, including any person on whose behalf the intermediary or electronic commerce service provider provides services in respect of information in an electronic record, for any action the intermediary or electronic commerce service provider takes in good faith in exercise of the powers conferred by, or as directed by, the Minister, under this section.

(5) Any person who lodges a notification of unlawful activity with an intermediary or electronic commerce service provider, knowing that it materially misrepresents the facts, commits an offence and is liable for damages for wrongful removal of the information or electronic record under subsections (1), (2) and (3).

Codes of conduct and standards for intermediaries and electronic commerce service providers.

**29.** (1) If a code of conduct is approved or a standard is specified by the Minister under this section to apply to intermediaries or electronic commerce service providers, those intermediaries or electronic commerce service providers shall comply with such code of conduct or standards, as the case may be.

(2) An intermediary or electronic commerce service provider who fails to comply with an approved code of conduct or specified standards, shall in the first instance be given a written warning by the Minister and the Minister may, direct that intermediary or electronic commerce service provider to cease and desist or otherwise to correct that intermediary's or electronic commerce service provider's practices within such period as may be specified in the direction.

(3) An intermediary or electronic commerce service provider, who fails to comply with a direction issued pursuant to subsection (2), commits an offence and is liable on summary conviction to a fine not exceeding fifty thousand dollars and if the offence is a continuing one to a further fine of one thousand dollars for each day the offence continues.

(4) If the Minister is satisfied that a body or organisation represents intermediaries or electronic commerce service providers, the Minister may by notice in writing, given to the body or organisation, direct the body or organisation to

- (a) develop a code of conduct that applies to intermediaries or electronic commerce service providers who deal with one or more specified matters relating to the provision of services by those intermediaries or electronic commerce service providers; and
- (b) provide a copy of that code of conduct to the Minister within such time as may be specified in the notice.

(5) If the Minister is satisfied with the code of conduct provided under subsection (4), the Minister shall approve the code of conduct by Notice published in the *Gazette* and thereupon the code of conduct shall apply to intermediaries or electronic commerce service providers, as the case may be, as may be specified in the Notice.

(6) If the Minister is satisfied that

- (a) no body or organisation represents intermediaries or electronic commerce service providers; or

- (b) a body or organisation to which notice is given pursuant to subsection (4) has not complied with the notice,

the Minister may, by Notice published in the *Gazette*, specify a standard that applies to the concerned intermediaries or electronic commerce service providers or both.

(7) If the Minister has approved a code of conduct or specified a standard that applies to intermediaries or electronic commerce service providers or both and

- (a) the Minister receives notice in writing, from a body or organisation representing intermediaries or electronic commerce service providers of proposals to amend the code of conduct or standard; or
- (b) the Minister no longer considers that the code of conduct or standard is appropriate,

the Minister may, by Notice published in the *Gazette*, revoke or amend the existing code of conduct or standard, as the case may be.

(8) References in this section to intermediaries or electronic commerce service providers include references to a particular class of intermediaries or electronic commerce service providers.

## PART VI MISCELLANEOUS

**30.** The Minister may, by Order, specify security procedure providers or classes of security procedure providers for the purposes of this Act.

Specified security procedure providers.

**31.** A person using electronic communications to sell goods or services to consumers shall provide

Information to be provided to consumers.

- (a) accurate, clear and accessible information about themselves, sufficient to allow
  - (i) the legal name of the person, its principal geographic address, and an electronic means of contact or telephone number;

- (ii) prompt, easy and effective consumer communication with the seller; and
- (iii) service of legal process;
- (b) accurate and accessible information describing the goods or services offered, sufficient to enable consumers to make an informed decision about the proposed transaction and to maintain an adequate record of the information; and
- (c) information about the terms, conditions and costs associated with a transaction, and notably
  - (i) terms, conditions and methods of payment; and
  - (ii) details of and conditions related to withdrawal, termination, return, exchange, cancellation and refund policy information.

Unwanted communications.

**32.** Any person who

- (a) sends unsolicited commercial communications electronically, to consumers based in the Virgin Islands; or
- (b) knowingly uses an intermediary or an electronic commerce service provider based in the Virgin Islands to send unsolicited commercial communications; or
- (c) has a place of business in the Virgin Islands and who sends, unsolicited electronic correspondence to consumers,

shall provide the consumer with a clearly specified and easily activated option to opt out of receiving future communications.

False or misleading information.

**33. (1)** A person who

- (a) files information required under this Act that contains false or misleading information;
- (b) provides a consumer or a user of an electronic signature with false or misleading information,

commits an offence.

- (2) A person who commits an offence under subsection (1) is liable on
  - (a) summary conviction to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding three years, or both; or
  - (b) conviction on indictment to a fine not exceeding two hundred thousand dollars or to imprisonment for a term not exceeding five years, or both.

**34.** Where an offence under this Act is committed by a body corporate, and is proved to have been committed with the consent or connivance of, or to be attributable to neglect on the part of, any director, manager, secretary or other similar officer of that body corporate, or a person purporting to act in that capacity, the person as well as the body corporate each commits the offence and are liable to be proceeded against and punished accordingly.

Offences by  
bodies  
corporate.

**35. (1)** The Minister may, with the approval of Cabinet, make Regulations for the giving effect to the provisions of this Act.

Regulations.

- (2) Without limiting the generality of subsection (1), Regulations may provide for
  - (a) the registering, licensing or accreditation of specified security procedure providers and their authorised representatives;
  - (b) prescribing the duties and liabilities of specified security procedure providers; and
  - (c) safeguarding or maintaining the effectiveness and efficiency of the common security infrastructure relating to the use of secure electronic signatures and the authentication of electronic records, including the imposition of requirements to ensure interoperability between specified security procedure providers or in relation to any security procedure;
  - (d) the use of certificates to support electronic signatures or authentication data;

- (e) the sale of goods or services by a person using electronic communications;
- (f) any forms and fees applicable for the purposes of this Act; and
- (g) prescribing anything that is required to be prescribed by this Act.

(2) Regulations made under subsection (1), may prescribe a fine not exceeding fifty thousand dollars or imprisonment for a term not exceeding twelve months or both, for any offence created under the regulations.

(3) Regulations made under subsection (1) shall be subject to a negative resolution of House of Assembly.

Repeal and savings.

**36.** (1) The Electronic Transactions Act is repealed.

No. 5 of 2001

(2) Any act, direction or thing duly done by any person under the repealed Act which is in force on the commencement date shall, on the commencement of this Act, be deemed to have been done under this Act to the extent of its consistency with this Act.

Passed by the House of Assembly this    day of                    , 2019.

Speaker.

Clerk of the House of Assembly.

## OBJECTS AND REASONS

The Bill seeks to enhance and modernise the legal framework relating to electronic transactions as is currently provided for in the Electronic Transactions Act 2001. In so doing, it would facilitate electronic governance by public authorities, as well as electronic commerce, by providing for the transfer of information and records by electronic means. It would also seek to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce and foster the development of electronic commerce through the use of secure electronic signatures to lend authenticity and integrity to correspondence in any electronic medium.

The Bill consists of six parts.

**Part I** (clauses 1 to 5) comprises the preliminary clauses.

**Clause 1** provides the short title and commencement of the proposed legislation.

**Clause 2** would define certain words and expressions used in the Bill.

**Clause 3** would provide that the Act binds the State.

**Clause 4** would make the Act inapplicable where the law requires writing, signatures or original documents in certain circumstances. These include the making, execution or revocation of a will; the conveyance or transfer of any interest in real property; the creation, performance or enforcement of an indenture of trust or power of attorney; the production of documents relating to immigration, citizenship or passport matters; or any other matters that may be prescribed by the Minister by Order.

**Clause 5** would provide for the autonomy of the parties concerned to use or accept electronic communications, electronic signatures and electronic contracts in certain circumstances.

**Part II** (clauses 6 to 15) would deal with the requirements for the legal recognition of electronic communications and records.

**Clause 6** would provide for the legal recognition of electronic communications.

**Clause 7** would provide that where a law requires any information or other matter to be in writing or in printed form that requirement is satisfied if the same is given, recorded or rendered electronically.

**Clause 8** would provide that where a law requires any information to be furnished in paper or other non-electronic form that requirement is satisfied if it is furnished electronically and is organised in substantially the same way and is accessible to

the other person so as to enable that person to retrieve or retain it for subsequent reference.

**Clause 9** would provide that where a law requires that access be provided to information in paper form, providing the information electronically would satisfy the requirement if the integrity of the information is maintained and the information is accessible.

**Clause 10** would provide that where any information is required by law to be delivered, dispatched, given, sent to or served on any person that requirement is satisfied if it is delivered, dispatched, given, sent to or served on that person by electronic medium and the originator of the electronic communication states that the receipt of the electronic communication is to be acknowledged and the addressee acknowledges receipt.

**Clause 11** would provide that where any information is required by law to be presented or retained in its original form that requirement is satisfied by presenting or retaining it by an electronic medium if there is reliability of accuracy of presentation and in its integrity in final electronic form.

**Clause 12** would provide for the retention of documents, records or information electronically where certain conditions are fulfilled including accessibility, accuracy, format, date and time of origin and destination of the electronic communication.

**Clause 13** would provide for several other requirements to allow for e-Commerce and e-Government.

**Clause 14** would provide for the comparison of an original document with the electronic form of that document where the electronic form of the document maintains the integrity of the original document.

**Clause 15** would provide for the admissibility of electronic communications that are reliable.

**Part III** (clauses 16 to 20) would provide for the formation and validity of electronic contracts.

**Clause 16** would provide for formation of contracts using electronic media, including the conclusion of contracts where the proposal is generally accessible to anyone, such as in online contracts where users of a website assent to the contract when visiting a website or when installing software.

**Clause 17** would provide for the recognition of a declaration of intent relating to electronic contracts.

**Clause 18** would provide for the establishment of the time and place of dispatch and receipt of electronic communications.

**Clause 19** would provide for the use of automated message systems for the formation of contracts.

**Clause 20** would provide for dealing with errors in partly automated transactions.

**Part IV** (clauses 21 to 26) would provide for the use of secure electronic signatures and secure electronic records.

**Clauses 21 and 22** would provide the use of electronic signatures in electronic transactions.

**Clause 23** would provide for the conduct of the signatory when using electronic signatures including, exercising reasonable care to avoid unauthorised use of his or her signature and notifying any person who may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if the signatory knows that the signature has been compromised, or there are circumstances which give rise to a substantial risk that the signature may have been compromised.

**Clause 24** would provide for the recognition of a certificate used to support an electronic signature and electronic signatures notwithstanding that they may be issued from a foreign jurisdiction.

**Clause 25** would provide for the recognition of an electronic record as secure where a specified security procedure or a commercially reasonable security procedure is used to verify the record. It would also provide for the verification of secure electronic signatures.

**Clause 26** would provide for certain presumptions relating to secure electronic records and signatures.

**Part V** (clauses 27 to 29) would set out the duties and liabilities of intermediaries and electronic commerce service providers.

**Clause 27** would provide for liability of intermediaries and electronic commerce service providers.

**Clause 28** would provide for the procedure for dealing with unlawful or defamatory information exchanged by intermediaries or electronic commerce service providers.

**Clause 29** would provide for the approval of the codes of conduct and specification of the standards required to be complied with by intermediaries and electronic commerce service providers. It would also provide for the penalties for

non-compliance with approved codes of conduct or specified standards by an intermediary or an electronic commerce service provider.

**Part VI** (clauses 30 to 36) would deal with miscellaneous matters including the regulation making power of the Minister, and the repeal of the Electronic Transactions Act 2001.

**Clause 30** would provide for the Minister to specify security procedure providers for the purposes of this Act.

**Clauses 31 and 32** would require persons using electronic communications to sell goods and services to provide certain information to consumers, as well as to protect consumers from unwanted electronic communications.

**Clause 33** would make it an offence to file or provide false or misleading information.

**Clause 34** would provide for offences by bodies corporate.

**Clause 35** would provide for the making of regulations and those regulations would be subject to a negative resolution of the House of Assembly.

**Clause 36** would provide for the repeal and savings.

Premier.