

A BILL

entitled

"THE ELECTRONIC TRANSACTIONS ACT 1999"

ARRANGEMENT OF SECTIONS

	PART I	16	Attribution of electronic records
	PRELIMINARY	17	Acknowledgement of receipt of electronic records
1	Citation	18	Time and place of dispatch and receipt of electronic records
2	Definitions		
3	Crown to be bound		
4	Objects		
5	Regulatory policy		
6	Exclusions		
7	Variation by agreement		
	PART II		
	LEGAL REQUIREMENTS RESPECTING ELECTRONIC RECORDS		
8	Legal recognition of electronic records	19	Electronic signature associated with accredited certificate
9	Writing	20	Certification and revocation of certification
10	Delivery	21	Recognition of external certification service providers
11	Signature	22	Pseudonyms
12	Original form	23	Liability of authorised certification service provider
13	Retention of electronic records		
14	Admissibility and evidential weight of electronic records		
	PART III		
	COMMUNICATION OF ELECTRONIC RECORDS		
15	Formation and validity of contracts		
			PART IV
			ELECTRONIC SIGNATURES
			PART V
			ENCRYPTION
		24	Regulations
		25	Amendments to the Criminal Code
			PART VI
			DATA PROTECTION
		26	Data protection

PART VII	PART VIII
INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS	E-COMMERCE ADVISORY BOARD
27 Liability of intermediaries	30 E-Commerce Advisory Board
28 Procedure for dealing with unlawful, defamatory etc. information	PART IX
29 Codes of conduct and standards for intermediaries and e-commerce service providers	GENERAL
	31 Offences, liability of corporate officers
	32 Regulations
	33 Consequential amendments
	34 Commencement
	SCHEDULE

WHEREAS it is expedient to make provision for electronic transactions and for matters connected therewith:

Be it enacted by The Queen's Most Excellent Majesty, by and with the advice and consent of the Senate and the House of Assembly of Bermuda, and by the authority of the same, as follows:—

PART I

PRELIMINARY

Citation

1 This Act may be cited as the Electronic Transactions Act 1999.

Definitions

2 In this Act—

"accredited certificate" means an electronic record that—

- (i) associates a signature verification device to a person;
- (ii) confirms the identity of that person;
- (iii) is issued by an authorised certification service provider; and
- (iv) meets the relevant criteria;

"addressee" in relation to an electronic record, means a person who is intended by the originator to receive the electronic

record, but does not include a person acting as an intermediary with respect to that electronic record;

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

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

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

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

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

"electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities;

"electronic agent device" means a program, or other electronic or automated means configured and enabled by a person that is used to initiate or respond to electronic records or performance in whole or in part without review by an individual;

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

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

- (i) it is uniquely linked to the signatory;
- (ii) it is capable of identifying the signatory;
- (iii) it is created using means that the signatory can maintain under his sole control; and
- (iv) it is linked to the information to which it relates in such a manner that any subsequent alteration of the information is revealed;

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

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

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

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

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

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

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

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

"prescribed" means prescribed by regulations under section 32;

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

"security procedure" means a procedure, established by law or agreement or knowingly adopted by each party, that is employed for the purpose of verifying that an electronic signature, record or performance is that of a particular person or for detecting changes or errors in the content of an electronic record;

"signature creation device" 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;

"signature verification device" means unique data, including codes or public cryptographic keys, or a uniquely configured physical device which is used in verifying an electronic signature;

Crown to be bound

3 (1) This Act binds the Crown.

(2) Notwithstanding subsection (1), nothing in this Act obliges any Government Department to generate, send, receive, store or otherwise process any record by electronic means, but the Minister may, by notice published in the Gazette, indicate that a Government Department will receive and process electronic records relating to such matters as may be specified in the notice.

Objects

4 The objects of this Act are—

- (a) to enhance the reputation of Bermuda as an international business centre;
- (b) to facilitate electronic transactions on a technology neutral basis by means of reliable electronic records;
- (c) to remove uncertainties in relation to conducting transactions electronically with respect to the requirements for documents and for signatures to be in writing;
- (d) to promote public confidence in the validity, integrity and reliability of conducting transactions electronically; and
- (e) to promote the development of the legal and business infrastructure necessary to implement electronic transactions securely.

Regulatory policy

5 Transactions carried out by electronic means shall be regulated in a manner that—

- (a) permits and encourages the growth of business by electronic means through the operation of free market forces;
- (b) promotes the greatest possible use of industry self-regulation;
- (c) is flexible; and
- (d) is technologically neutral.

Exclusions

6 (1) Part II (legal requirements respecting electronic records) and Part III (communication of electronic records) do not apply to any rule of law requiring writing or signatures for the following matters—

- (a) the creation, execution or revocation of a will or testamentary instrument;
- (b) the conveyance of real property or the transfer of any interest in real property.

(2) The Minister may by regulations provide that this Act, or such provisions thereof as may be specified in the regulations, does not apply to any class of transactions, persons, matters or things specified in the regulations.

Variation by agreement

7 As between parties involved in generating, sending, receiving, storing or otherwise processing records, any provision of Part II (legal requirements respecting electronic records) or Part III (communication of electronic records) may be varied by agreement.

PART II

LEGAL REQUIREMENTS RESPECTING ELECTRONIC RECORDS

Legal recognition of electronic records

8 Information shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is—

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

Writing

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

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

Delivery

10 (1) Where information is required by law to be delivered, dispatched, given or sent to, or to be served on, a person, that requirement is met by doing so in the form of an electronic record provided that the originator of the electronic record states that the receipt of the electronic record is to be acknowledged and the addressee has acknowledged its receipt.

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

Signature

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

- (a) a method is used to identify that person and to indicate that the person intended to sign or otherwise adopt the information in the electronic record; and
- (b) that method is as reliable as is appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) An electronic record that meets the requirements of subsection (1)(a) and (b) shall not be denied legal effect, validity and enforceability solely on the ground that it—

- (a) is not an electronic signature; or
- (b) is not associated with an accredited certificate.

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

Original form

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

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

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

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

- (a) the criterion for assessing integrity is whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

- (b) the standard of reliability required is to be assessed in the light of the purpose for which the information was generated and all the relevant circumstances.

Retention of electronic records

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

- (a) the information contained in the electronic record is accessible and is capable of retention for subsequent reference;
- (b) the electronic record is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
- (c) any information that enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received is retained.

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

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

Admissibility and evidential weight of electronic records

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

- (a) solely on the ground that it is an electronic record; or
- (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the ground that it is not in its original form.

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

- (a) the reliability of the manner in which the electronic record was generated, stored or communicated;
- (b) the reliability of the manner in which the integrity of the information was maintained;
- (c) the manner in which the originator was identified; and
- (d) any other relevant factor.

(3) This section does not affect the application of sections 27E, 27F, 43A and 43B of the Evidence Act 1905 (which relate to the admissibility of documents produced by computers).

PART III

COMMUNICATION OF ELECTRONIC RECORDS

Formation and validity of contracts

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

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

Attribution of electronic records

16 (1) An electronic record is attributable to a person if the electronic record resulted from the action of the person, acting in person, by his agent, or by his electronic agent device.

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

(3) Attribution of an electronic record by a person under this section has the effect provided for by the law, regulation, or agreement regarding the security procedure.

Acknowledgement of receipt of electronic records

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

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

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

(b) any conduct of the addressee,

that is reasonably sufficient to indicate to the originator that the electronic record has been received.

(3) Where the originator has stated that the electronic record is conditional on receipt of the acknowledgement, the electronic record is to

be treated as though it had never been sent until the acknowledgement is received.

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

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

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

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

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

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

Time and place of dispatch and receipt of electronic records

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

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

(a) where the addressee has designated an information processing system for the purpose of receiving electronic records, receipt occurs—

(i) at the time when the electronic record enters the designated information processing system; or

(ii) if the electronic record is sent to an information processing system of the addressee that is not the designated information processing system,

at the time when the electronic record comes to the attention of the addressee;

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

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

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

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

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

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

PART IV

ELECTRONIC SIGNATURES

Electronic signature associated with an accredited certificate

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

Certification and revocation of certification

20 (1) The provision of certification services for electronic signatures is not subject to prior authorisation.

(2) The Minister, on application by a certification service provider and on payment of such fee as may be prescribed under the Government Fees Act 1965, may, if satisfied that the applicant meets the relevant criteria (which may include criteria in respect to electronic

signature products), by notice published in the Gazette, authorise the applicant to provide accredited certificates.

(3) Subject to subsection (4), the Minister, if satisfied that an authorised certification service provider no longer meets the relevant criteria, may by notice published in the Gazette revoke an authorisation given under subsection (2).

(4) Before revoking an authorisation under subsection (3), the Minister shall give notice in writing to the authorised certification service provider of his intention to do so and indicating his reasons for the proposed revocation and shall invite the authorised certification service provider, within 14 days of the notice, to submit representations in writing as to why the authorisation should not be revoked, and the Minister shall consider those representations.

(5) In this section the "relevant criteria" means such policy criteria as the Minister may specify by notice published in the Gazette.

Recognition of external certification service providers

21 (1) The Minister may by notice published in the Gazette, recognise certificates or classes of certificates issued in, or certification service providers or classes of certification service providers established in any other jurisdiction and, upon such recognition and on payment of such fee as may be prescribed under the Government Fees Act 1965—

- (a) those certificates or classes of certificates shall be deemed to be accredited certificates; and
- (b) those certification service providers or classes of certification service providers shall be deemed to be authorised under subsection 20(2).

(2) In determining to accord recognition under subsection (1) the Minister shall have regard to whether—

- (a) the certificates or classes of certificates are required to, and do in fact, meet obligations equivalent to those required for an accredited certificate; and
- (b) the certification service providers or classes of certification service providers are required to, and do in fact, meet criteria equivalent to those required for an authorised certification service provider.

(3) The Minister may, by notice published in the Gazette, revoke any recognition accorded under subsection (1), but, before doing so, the Minister shall advise the person affected of his intention to do so and indicating his reasons for the proposed revocation and shall invite that person, within 14 days of the notice, to submit representations in writing as to why the recognition should not be revoked, and the Minister shall consider those representations.

Pseudonyms

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

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

(3) Where personal data is transferred pursuant to subsection (2), the certification service provider shall make a record of the transfer and as soon as possible thereafter give notice to the signatory of the transfer.

Liability of authorised certification service provider

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

- (a) the accuracy of all information in the accredited certificate as from the date on which it was issued, unless the authorised certification service provider has stated otherwise in the accredited certificate;
- (b) assurance that the person identified in the accredited certificate held, at the time the accredited certificate was issued, the signature creation device corresponding to the signature verification device given or identified in the accredited certificate;
- (c) if the authorised certification service provider generates both the signature creation device and the signature verification device, assurance that the two devices function together in a complementary manner,

unless the person who relied on the accredited certificate knows or ought reasonably to have known that the authorisation of the certification service provider has been revoked.

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

- (a) the information was provided by or on behalf of the person identified in the accredited certificate; and
- (b) the certification service provider can demonstrate that he has taken all reasonably practical measures to verify that information.

(3) An authorised certification service provider that—

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

(b) makes those limits known to third parties,

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

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

PART V

ENCRYPTION

Regulations

24 (1) The Minister may make regulations—

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

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

(2) For the avoidance of doubt it is declared that, subject to any regulations made under subsection (1), it is lawful in Bermuda for a person to use any encryption program or other encryption product of any bit size or other measure of the strength of the encryption provided that it has lawfully come into the possession of that person.

Amendments to the Criminal Code

25 Section 464 of the Criminal Code Act 1907 is amended—

(a) in subsection (1), by inserting after the words "any such thing" the words ", together with any device, computer program or information necessary to secure access to, or to comprehend the meaning of, such thing or its contents";

(b) by inserting the following after subsection (1)—

" (1A) If it appears to a magistrate or to a Justice of the Peace, on complaint made on oath, that there are reasonable grounds for suspecting that a person is in possession of information or of a computer, computer program on any similar device which is relevant to the interpretation of any thing seized under subsection (1), then the magistrate or Justice of the Peace may direct that person to assist a police officer in the manner provided in subsection (7)."

(c) by the addition of the following:

" (6) If the thing seized under a warrant issued under subsection (1) is a computer, computer program, or any other similar device, the magistrate may direct that a police officer be permitted to make copies of any information, software or data required for the investigation or prosecution of an offence and may direct any person arrested in connection with the warrant pursuant to which the computer, computer program or other similar device was seized to disclose or execute any procedure necessary to render the contents of the computer intelligible.

(7) If any other person is in possession of the devices, procedures or information necessary to render intelligible the contents of a computer, computer program, or any other similar device, for the purposes of subsection (6), then the magistrate may by direction pursuant to subsection (1A), require such person to surrender or provide copies of such devices or information or to execute such procedures.

(8) Any person who fails to comply with a direction under subsection (1A), (6) or (7) is guilty of an offence and is liable on summary conviction to imprisonment for 6 months or to a fine of \$50,000, or to both."

PART VI

DATA PROTECTION

Data protection

26 (1) The Minister may make regulations prescribing standards for the processing of personal data whether or not the personal data originates inside Bermuda.

(2) The regulations may provide for—

- (a) the voluntary registration and de-registration to the standards by data controllers and data processors;
- (b) the establishment of a register that is available for public inspection showing particulars of data controllers and data processors who have registered or de-registered to the standards and the dates thereof and the countries in respect of which the registration applies;
- (c) the application of the standards to those countries specified in the regulations;
- (d) different standards to be applied in respect of personal data originating from different countries.

(3) A data controller or data processor who voluntarily registers to a standard in subsection (1) must comply with the standard, as it may be amended from time to time, in respect to any personal data originating from a country to which the standard applies that is collected by the data controller during the period of registration, including any time after de-registration, and, if he fails to do so, is guilty of an offence and is liable on summary conviction to imprisonment for 6 months or to a fine of \$50,000, or to both.

PART VII

INTERMEDIARIES AND E-COMMERCE SERVICE PROVIDERS

Liability of intermediaries

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

- (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—
 - (i) acquires knowledge that the information gives rise to civil or criminal liability; or
 - (ii) becomes aware of facts or circumstances from which the likelihood of civil or criminal liability in respect of the information ought reasonably to have been known.

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

(3) Nothing in this section relieves an intermediary from complying with any court order, injunction, writ, Ministerial direction, regulatory requirement, or contractual obligation in respect of an electronic record.

Procedure for dealing with unlawful, defamatory etc. information

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

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

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

- (a) follow the relevant procedure set out in a code of conduct approved or standard appointed under section 29 if such code or standard applies to the intermediary; or
- (b) notify the Minister.

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

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

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

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

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

(2) An intermediary or e-commerce service provider who fails to comply with an approved code of conduct or appointed standard, shall in the first instance be given a written warning by the Minister and the Minister may direct that person to cease and desist or otherwise to correct his practices, and, if that person fails to do so within such period as may be specified in the direction, he shall be guilty of an offence and be liable on summary conviction to a fine of \$5,000 for each day on which the contravention continues.

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

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

(4) If the Minister is satisfied with the code of conduct provided under subsection (3), the Minister shall approve the code of conduct by notice published in the Gazette and thereupon the code of conduct applies to intermediaries or e-commerce service providers as may be specified in the notice.

(5) If the Minister is satisfied that—

- (a) no body or organization represents intermediaries or e-commerce service providers; or
- (b) a body or organization to which notice is given under subsection (3) has not complied with the request of the Minister under that subsection,

the Minister may, by notice published in the Gazette, appoint a standard that applies to intermediaries or e-commerce service providers.

(6) If the Minister has approved a code of conduct or appointed a standard that applies to intermediaries or e-commerce service providers and—

- (a) the Minister receives notice from a body or organization representing intermediaries or e-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 any existing code of conduct or standard.

- (7) A code of conduct approved or standard appointed under this section may relate to one or more of the following matters—
- (a) the types of services and of customers that are permitted to be provided services by intermediaries;
 - (b) the types of information permitted to be contained in electronic records for which services are provided by intermediaries;
 - (c) the contractual application of relevant codes of conduct or standards to customers of intermediaries and e-commerce service providers;
 - (d) information to be disclosed by intermediaries and e-commerce service providers including name, address, e-mail address and contact and registration details;
 - (e) the use of a quality accreditation mark associated with Bermuda;
 - (f) the actions to be taken in the event of customers of intermediaries or e-commerce service providers sending bulk, unsolicited electronic records;
 - (g) business activities prohibited by the Tenth Schedule to the Companies Act 1981;
 - (h) publication of material that contravenes the Obscene Publications Act 1973 or the Criminal Code Act 1907;
 - (i) procedures for dealing with complaints;
 - (j) procedures for dispute resolution, including dispute resolution by electronic means;
 - (k) such other matters as the Minister may require.
- (8) References in this section to intermediaries and e-commerce service providers include reference to a particular class of intermediary and a particular class of e-commerce service provider respectively.

PART VIII

E-COMMERCE ADVISORY BOARD

E-Commerce Advisory Board

30 (1) There shall be a board to be known as the "E-Commerce Advisory Board" for the purpose of providing advice to the Minister on matters connected with the discharge of his functions under this Act.

(2) The Minister shall appoint the members of the Board by notice published in the Gazette.

(3) The Board shall consist of not fewer than 5 nor more than 11 persons appearing to the Minister to be knowledgeable about electronic commerce or international business.

(4) The Minister shall designate one of the persons appointed a member under subsection (2) to be the chairman of the Board.

(5) The Board shall determine its own procedure.

(6) The function of the Board is to advise the Minister on any matter referred to it by the Minister, or which, of its own initiative, the Board considers appropriate.

PART IX

GENERAL

Offences, liability of corporate officers

31 Where a corporation is guilty of an offence under this Act or regulations made under this Act, every person who at the time of the commission of the offence was a director or officer of the corporation is guilty of the like offence unless he proves that the contravention took place without his consent or that he exercised all due diligence to prevent the commission of the offence.

Regulations

32 (1) The Minister may make regulations generally for any matter the Minister considers necessary to give effect to this Act and, in particular,—

- (a) prescribing the relevant criteria for the issue of an accredited certificate;
- (b) respecting any matter for which provision may be made by regulations under this Act.

(2) The regulations may provide that any contravention of a provision thereof constitutes an offence and may prescribe a penalty for that offence.

(3) Regulations made under subsection (1) are subject to the negative resolution procedure.

Consequential amendments

33 The Acts set out in column 1 of the Schedule are amended in the manner set out in column 2 of that Schedule.

Commencement

34 This Act or any provision thereof comes into operation on such day as the Minister may appoint by notice published in the Gazette.

SCHEDULE

(section 33)

Arbitration Act 1986

section 20

Insert after subsection (1) the following—

" (1A) For the purposes of subsection (1) the examination of witnesses on oath or affirmation and the administering of oaths or the taking of affirmations of witnesses in the arbitration may be conducted by appropriate electronic means."

**Bermuda International
Conciliation and
Arbitration Act 1993**

section 7

Insert next after subsection (3) the following—

" (4) For the purposes of subsection (2)—

- (a) discussions with one or more parties;
- (b) the hearing of witnesses, experts or parties;
- (c) the inspection of documents, goods or other property; and
- (d) consultation with the conciliator,

may, as far as is practicable, be conducted by electronic means and the conciliator and one or more of the parties are not required to be physically present in the same place at any time."

**Computer Misuse Act
1996**

section 6

Insert next after section 6 the following—

"Causing computer to cease to function

6A (1) A person is guilty of an offence if—

(a) he causes a computer to cease to function permanently or temporarily; and

(b) at the time he engages in conduct that causes a computer to cease to function permanently or temporarily he has—

(i) knowledge that the conduct is unauthorised;

(ii) the requisite knowledge; and

(iii) the requisite intent.

(2) For the purposes of subsection (1)(b)—

(a) "requisite knowledge" is knowledge that the conduct would or would be likely to cause a computer to cease to function permanently or temporarily; and

(b) "requisite intent" is intent to cause a computer to cease to function and by so doing—

- (i) prevent or hinder access to the computer;
or
- (ii) impair the operation of the computer,

but the intent need not be directed at a particular computer.

(3) A person guilty of an offence under this section is liable—

- (a) on summary conviction to imprisonment for 6 months or to a fine of \$6,000 or to both;
- (b) on conviction or indictment to imprisonment for 5 years or to a fine of \$20,000 or to both."

section 7

In subsection (1), delete "or 5" and substitute ", 5 or 6A".

Insert next after subsection (3) the following:

" (3A) "Significant link", in relation to an offence under section 6A, means—

- (a) that the accused was in Bermuda when he engaged in conduct which caused the computer to cease to function permanently or temporarily;
or
- (b) that the computer was in Bermuda."

**Exempted Partnerships
Act 1992**

section 19

Insert next after subsection (2) the following—

" (2A) Nothing in subsection (1)(e) shall prohibit an exempted partnership from offering goods or services electronically from a place of business in Bermuda or through an internet or other electronic service provider located in Bermuda."

**Government Authorities
(Fees) Act 1971**

First Schedule

Insert after the entry relating to the Development Applications Board the following—

"E-Commerce Advisory Board established under section 30 of the Electronic Transactions Act 1999".

Interpretation Act 1951

section 7(1)

Insert after the definition of "public place" the following—

"record" includes a record created, stored, generated, received or communicated by electronic, magnetic, optical or other similar means;"

**Overseas Partnerships
Act 1995**

section 11

Insert next after subsection (2) the following—

" (2A) Nothing in subsection (1)(e) shall prohibit an overseas partnership from offering goods or services electronically

from a place of business in Bermuda or through an internet or other electronic service provider located in Bermuda.

(2B) An overseas partnership shall be deemed to engage in or carry on any trade or business in Bermuda if it makes known by way of advertisement or by any statement on a web site or by an electronic record as defined in the Electronic Transactions Act 1999 that it may be contacted at a particular address in Bermuda or if it uses a Bermudian domain name."

ELECTRONIC TRANSACTIONS BILL 1999

EXPLANATORY MEMORANDUM

The Bill establishes the legal principles for the conduct of electronic commerce and the processing of electronic transactions. The Bill draws upon a variety of sources including the UNCITRAL Model Law on Electronic Commerce (Parts II and III), the European Parliament and Council directive for a common framework for electronic signatures (Part IV), the safe harbour principles of the European Union relating to data protection (Part VI) and the legislation of other jurisdictions, notably that of Singapore.

The Bill lays a foundation for the conduct of electronic transactions on a technology-neutral basis that is sufficiently flexible to embrace new technological developments and that contemplates a high degree of self-regulation.

Clause 1 is the standard citation provision.

Clause 2 sets out the definitions of terms and expressions used in the Bill.

Clause 3 recites that the Bill applies to the Crown and enables the Minister by notice in the Gazette to indicate when and in relation to what matters a Government Department will receive and process records in electronic form.

Clause 4 sets out the objects of the Bill which include the enhancement of the reputation of Bermuda as an international business centre.

Clause 5 indicates the regulatory policy to be applied by the Minister in administering the Bill.

Clause 6 excludes the application of Parts II and III to wills and conveyances of real property, and the existing legal formalities and requirements for writing will continue to apply to them.

The Minister may by regulations provide that parts of the Bill do not apply to particular matters or transactions identified in the regulations.

Clause 7 enables the parties to a transaction by agreement to vary the application of Parts II and III.

Clause 8 is based on Article 5 of the Model Law and sets out the fundamental principle that an electronic record is not subject to legal challenge merely because it is in electronic form.

Clause 9 is based on Article 6 of the Model Law and provides that a legal requirement for writing is satisfied by an electronic record if the record is accessible and capable of retention for subsequent reference.

Clause 10 provides that if information is required by law to be delivered or sent to a person it may be delivered or sent by electronic means.

Clause 11 is based on Article 7 of the Model Law and provides that, where a signature is required by law, an electronic record meets that requirement if the method of identifying the signatory meets certain requirements.

Clause 12 is based on Article 8 of the Model Law and sets out the minimum requirements for an electronic record to be regarded as the functional equivalent of an original.

Clause 13 is based on Article 10 of the Model Law and sets out the requirements for the storage of documents, information or records in electronic form.

Clause 14 is based on Article 9 of the Model Law and provides that an electronic record will not be denied admissibility in evidence solely on the ground that it is in electronic form or that, if it is the best evidence, on the ground that it is not in the original form.

Clause 15 is based on Article 11 of the Model Law and provides that in the context of contract formation the fact that the transaction is conducted in electronic form does not affect its validity.

Clause 16 deals with attribution of electronic records and provides that an electronic record is attributed to a particular person if it resulted from an action of that person or through an agent or electronic agent of that person.

Clause 17 is based on Article 14 of the Model Law and deals with acknowledgement of receipt of electronic records and sets out rules to be applied in situations where the parties have agreed a form of acknowledgement, and where they have not.

Clause 18 is based on Article 15 of the Model Law and sets out rules governing the dispatch and receipt of electronic records and adopts the principle that the place of business of each of the parties is the governing criterion rather than the location of the information processing system.

Clause 19 provides that where an electronic signature is associated with an accredited certificate it is deemed to satisfy the requirements of an electronic signature set out in Clause 11.

Clause 20 enables the Minister to authorise a certification service provider who meets the policy criteria that the Minister will specify by notice in the Gazette to issue accredited certificates which confirm the veracity of an electronic signature.

Clause 21 enables the Minister to recognise certificates and certification service providers in any other jurisdiction and, upon recognition, the certificates are to be treated as equivalent to accredited certificates issued in Bermuda.

Clause 22 enables pseudonyms to be used as electronic signatures subject to the right of the certification service provider, when required by law, to reveal the identity of the electronic signatory.

Clause 23 provides that an authorised certification service provider is liable to any person who reasonably relies on an accredited certificate for the accuracy of the information in the certificate and for assurance that the person

identified in the certificate held a signature creation device corresponding to the signature verification device identified in the certificate. However, the service provider is not liable for errors where the information was provided by or on behalf of the person to whom the certificate was issued.

Clause 24 empowers the Minister to make regulations relating to the use, import and export of encryption programs and other encryption products.

The clause recites that it is lawful in Bermuda to use encryption programs that have lawfully come into the possession of the user.

Clause 25 makes amendments to the Criminal Code to enable the police to seize encryption software and to empower a magistrate to direct persons to provide assistance necessary to decode encrypted information.

Clause 26 enables the Minister to make regulations with respect to the protection of personal data.

The aim of the provisions is to create a regime consistent with the European Union's "safe harbour" principles for the transfer of personal data outside the European Union.

Clause 27 recognises that an intermediary, who merely provides a conduit, should not be liable for the content of electronic records if the intermediary has no actual knowledge or is not aware of facts that would objectively indicate a likelihood of civil or criminal liability in respect of material on the intermediary's network.

Clause 28 sets out a procedure that intermediaries must follow if they become aware of facts or circumstances that give rise to civil or criminal liability in respect of information on their networks. The intermediary must remove the offensive material and notify the Minister of the identity of the client. The Minister may issue directions to require the intermediary to withdraw service to the client.

Clause 29 establishes a mechanism for the creation of codes of conduct or standards to be applied to intermediaries and e-commerce service providers. The intention is that a code of conduct will be developed by the industry, but if it fails to do so, the Minister may intervene and establish a standard.

The matters that may be included in a code of conduct or standard are set out in subsection (7) and include prohibited business activities, spamming, complaints and on-line dispute resolution procedures.

Clause 30 provides for the establishment of the E-Commerce Advisory Board to guide the Minister on the exercise of the Minister's functions.

Clause 31 imposes liability on corporate officers for offences committed under this Act.

Clause 32 provides general authority to make regulations subject to the negative resolution procedure.

Clause 33 introduces the amendments to various Acts that are set out in the Schedule.

The amendments to the Companies Act 1981 require that an overseas company which holds itself out as carrying on business in Bermuda by using a

Bermuda address or Bermudian domain name must obtain a permit but an exempted company which merely offers goods and services electronically from a place of business or through a Bermuda website will not be regarded as carrying on business in Bermuda.

Similar amendments are made in relation to the law governing exempted and overseas partnerships.

The amendments to the Bermuda International Conciliation and Arbitration Act 1993 and the Arbitration Act 1986 provide for the conduct of arbitration and conciliation proceedings using electronic communications.

The amendments to the Computer Misuse Act 1996 are to create a new offence of causing a computer to cease to function permanently or temporarily when done with the requisite knowledge and intent.

The amendment to the Interpretation Act 1951 is to create a definition of "record" to include electronic records.

Clause 34 provides for any provision of the Bill to come into operation on a date specified by the Minister by notice in the Gazette.