Supplement No. 2 published with Gazette No. 15 of 28th July, 2003

ELECTRONIC TRANSACTIONS LAW

(2003 Revision)

Law 7 of 2000 consolidated with Law 4 of 2002 (part).

Revised under the authority of the Law Revision Law (1999 Revision).

Originally enacted –

Law 7 of 2000-20th July, 2000
Law 4 of 2002-18th March, 2002

Consolidated and revised this 10th day of June, 2003.

ELECTRONIC TRANSACTIONS LAW

(2003 Revision)

ARRANGEMENT OF SECTIONS

Part 1 - Introductory

Part II - Legal Requirements Respecting Electronic Records

Part III - Formation and Validity of Contracts

Part IV - Communication of Electronic Records

Part V - Electronic Signatures

Part VI - Information Security Service Providers

Part VII - Intermediaries and E-Commerce Service Providers

Part VIII - Data Protection

Part IX – Miscellaneous

ELECTRONIC TRANSACTIONS LAW

(2003 Revision)

PART 1 – Introductory

1. This Law may be cited as the Electronic Transactions Law (2003 Revision). Short title

2. In this Law - Definitions

"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;

"Authority" means the Information and Communications Technology (ICT) Authority established by section 3 of the Information and Communications Technology Law, 2001; Law 4 of 2002

"Board" means the e-Business Advisory Board appointed under section 39;

"certificate" means an electronic record which purports to ascertain the identity of a person or entity who, at the time of creation of that record, controls a particular signature device;

"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, stored, altered, transmitted, distributed or otherwise processed;

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

"deliver" includes give, serve and file;

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

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

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

"electronic record" means a record processed and maintained by electronic means;

"electronic signature" means an electronic sound, symbol or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign the electronic record;

"Governor", except in the definition "ministry or portfolio", means Governor in Council;

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

"information processing system" means an electronic system for processing information;

"information security service" and "information security procedure" includes a service or procedure which is provided to an originator, intermediary or recipient of an electronic record, and which is designed to -

(a) secure that that record can be accessed, or can be put into an intelligible form, only by certain persons; or

(b) secure that -

(i) the authenticity;

(ii) the time of processing; or

(iii) the integrity,

of such a record is capable of being ascertained;

"intermediary", with respect to an electronic record, means a person who processes that electronic record for another person;

"Minister" means the minister for the time being responsible for commerce;

"ministry or portfolio" includes the office of the Governor, the office of the Auditor-General and the courts' administrative service;

"originator", in relation to an electronic record, means a person who -

(a) sends an electronic record;

(b) instructs another to send an electronic record on his behalf; or

(c) has an electronic record sent by his electronic agent,

but does not include -

(i) a person who sends an electronic record on the instructions of another; or

(ii) a person acting as an intermediary with respect to that electronic record;

"personal data" means data which relate to a person who can be identified -

(a) from those data; or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes any expression of opinion about that person and any indication of the intentions of the data controller or any other person in respect of that person;

"prescribed" means prescribed in regulations made by the Governor;

"process", in relation to an electronic record, means create, generate, send, transmit, receive, store, communicate, modify or display the record;

"record" means information that is inscribed, stored or otherwise maintained on a tangible medium or that is stored in an electronic or any other medium and is accessible in a perceivable form;

"signature device" means unique data or a uniquely configured physical device, which is used by the signatory for the purposes of creating an electronic signature; and

"transaction" means a transaction whether or not for consideration and whether or not of a commercial nature.

Exclusions

3. (1) This Law shall not apply to any rule of law requiring writing or signatures for the creation, execution, variation or revocation of a will or other testamentary instrument.

(2) The Governor may provide, by regulations subject to affirmative resolution, that this Law, or such of its provisions as may be specified in the regulations, shall not apply to any class of transactions, persons, matters or things.

Variation by agreement

4. The provisions of Part II, so far as they relate to a contract or deed, (except section 15(b) and (c) and Parts III, IV and V (except sections 20 and 22(2) to (6) may be varied or excluded by agreement.

Crown to be bound

5. (1) This Law binds the Crown.

(2) Notwithstanding subsection (1), nothing in this Law shall require a ministry or portfolio to process an electronic record, but either the Minister or the appropriate minister or official member may, by notice published in the Gazette, indicate that a ministry or portfolio will process electronic records relating to such matters as may be specified in the notice.

(3) Until a notice under subsection (2) is published, no person dealing with such ministry or portfolio shall be entitled, by means of an electronic record, to satisfy a requirement to process a record.

Part II - Legal Requirements Respecting Electronic Records

Legal recognition of electronic record

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

(a) in the form of an electronic record; or
(b) referred to but not contained in an electronic record.

Writing

7. (1) Where a document, record or information is required or permitted by any statutory provision, rule of law, contract or deed to be in writing, or is described in any statutory provision or contract as being written, that requirement, permission or description may be met by information in the form of an electronic record.

(2) Subsection (1) shall apply if the requirement for the document, record or information to be in writing is in the form of an obligation or if the statutory provision, rule of law, contract or deed provides consequences if it is not in writing.

Delivery

8. (1) Where a document, record or information is required or permitted by any statutory provision, rule of law, contract or deed to be delivered or sent to a person, that requirement or permission may be met by delivery of it in the form of an electronic record if -

(a) the format of the electronic record and the means of delivery is acceptable to the parties; and
(b) where the originator of the electronic record states that the receipt of the electronic record is to be acknowledged, the addressee has knowingly acknowledged the receipt.

(2) Subsection (1) applies whether or not the requirement for delivery or sending is in the form of an obligation or whether or not the statutory provision, rule of law, contract or deed provides consequences for the document, record or information not being delivered or sent.

Original form

9. (1) (a) Where a statutory provision, rule of law, contract or deed requires conclusive evidence of the original form of a document, record or information to be presented or retained, that requirement shall be met by the presentation or retention of an electronic record if the document, record or information is accurately represented therein.

(b) Paragraph (a) shall apply if the requirement for the presentation or retention of evidence of the original form of document, record or information is in the form of an obligation or if the statutory provision, rule of law, contract or deed provides consequences if

conclusive evidence of the original form of document, record or information is not provided.

(2) (a) Where a statutory provision, rule of law, contract or deed requires a document, record or information to be presented or retained in its original form and such document, record or information was first generated in its final form as an electronic record, that requirement shall be met by the presentation or retention of an electronic record if the document, record or information is accurately represented therein.

(b) Paragraph (a) shall apply if the requirement to present or retain the document, record or information in its original form is in the form of an obligation or if the statutory provision, rule of law, contract or deed provides consequences if the original form of the document, record or information is not presented or retained.

(3) For the purposes of subsections (1) and (2), the document, record or information is accurately represented where it has remained complete and unaltered from the time it was first generated in its final form, whether as an electronic record or on any other medium, apart from the application of an information security procedure, or apart from -

(a) the addition of an endorsement; or

(b) an immaterial change,

which arises in the normal course of communication, translation, conversion, storage or display.

Retention of records

10. (1) Where documents, records or information are required by any statutory provision, rule of law, contract or deed to be retained, that requirement is met by retaining them in the form of electronic records if -

(a) the information contained in the electronic record is accessible and 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 document, record or information when it was 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 and received is retained.

(2) An obligation to retain documents, records or information, under subsection (1) does not extend to 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 another person, if the conditions set out in subsection (1)(a), (b) and (c) are met.

Records available for inspection

11. Where documents, records or information are required by any statutory provision, rule of law, contract or deed to be made available for inspection, that requirement shall be met by making such documents, records or information available for inspection in perceivable form as an electronic record.

Admissibility of electronic records

12. 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 an electronic record or an electronic signature.

Part III - Formation and Validity of Contracts

Formation and validity of contracts

13. (1) In the context of the formation of a contract -

(a) an offer;
(b) subject to any condition included in the offer (notwithstanding section 4), the acceptance of an offer; and
(c) the method of payment of any consideration payable,

may be expressed by an electronic record.

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

Part IV - Communication of Electronic Records

Attribution of electronic records

14. (1) An electronic record is that of an originator if it was sent by the originator himself.

(2) As between the originator and the addressee, an electronic record shall be attributable to the originator if it was sent -

(a) by a person who had been authorised by the originator to send the electronic record on his behalf; or
(b) by the originator's electronic agent.

(3) As between the originator and the addressee, an addressee shall be entitled to attribute an electronic record to the originator, and to act on that assumption, if -

(a) in order to ascertain whether the electronic record was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the electronic record as received by the addressee resulted from the actions of a person whose relationship with the originator, or with any agent of the originator, enabled that person to gain access to a method used by the originator to identify electronic records as his own.

(4) Subsection (3) does not apply -

(a) as of the time when the addressee has both received notice from the originator that the electronic record is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case to which subsection (3)(b) applies, at any time when the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, that the electronic record was not that of the originator.

(5) The addressee shall be entitled to regard each electronic record received as a separate electronic record and to act on that assumption, except to the extent that it duplicates another electronic record and the addressee knew or should have known, had he exercised reasonable care or used any agreed procedure, that the electronic record was a duplicate.

Effect of change or error

15. If a change or error occurs in the transmission of an electronic record -

(a) if the originator and the addressee have agreed to use an information security procedure in respect of the electronic record and one of them has conformed to the procedure, but the other has not, and the nonconforming person would have detected the change or error had he also conformed, the conforming person may avoid the effect of the changed or erroneous electronic record;

(b) if an individual is either the originator or the addressee of an electronic record, he may avoid the effect of the electronic record if the error was made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual-

(i) promptly notifies the other person of the error and that he did not intend to be bound by the electronic record received by the other person;

(ii) takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and

(iii) has not used or received any benefit or value from the consideration, if any, received from the other person; and

(c) if neither paragraph (a) nor paragraph (b) applies, the change or error shall have the effect provided by any other law and any contract between the originator and the addressee.

Acknowledgement of receipt of electronic records

16. (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 agreed with, the addressee that receipt of the electronic record be acknowledged by the addressee.

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

(b) 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 an electronic record is conditional on receipt by him of an acknowledgement, the electronic record shall be presumed not to have been sent until an acknowledgment has been received by him.

(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 -

(i) stating that no acknowledgement has been received and that the electronic record is to be treated as though it had never been sent; or

(ii) 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 -

(i) treat the electronic record as though it had never been sent; and

(ii) exercise any other rights the originator may have.

(5) Where the originator receives the addressee's acknowledgement of receipt it may be presumed that the related electronic record has been received by the addressee but that presumption shall not imply that the electronic record received corresponds to the electronic record as sent.

(6) Where the addressee's received acknowledgment states that the related electronic record met technical requirements that the originator and the addressee have agreed should be met, it shall be presumed that the requirements have been met.

(7) Except insofar as it relates to the sending or receipt of an electronic record, this section shall not affect the legal or equitable consequences that may flow either from that electronic record or from the acknowledgement of its receipt.

Time and place of sending and receipt of electronic records

17. (1) An electronic record which is transmitted by electronic means is sent at the time when it enters an information processing system outside the control of the originator, his agent, his electronic agent, or his agent's electronic agent.

(2) An electronic record which is transmitted by electronic means is received -

(a) in the case where the addressee has designated an information processing system for the purpose of receiving an electronic record -

(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 is retrieved by the addressee; or

(b) in the case where the addressee has not designated an information processing system, at the time when the electronic record enters an information processing system of the addressee or is otherwise retrieved by 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) Subject to subsection (6), an electronic record shall be deemed to have been sent at the place where the originator or his agent has his place of business, and shall be deemed to have been received at the place where the addressee or his agent has his place of business.

(5) For the purposes of subsection (4), if the originator or the addressee has more than one place of business, his place of business is -

(a) that place of business which has the closest relationship to the transaction to which the electronic record relates; or
(b) where there is no transaction to which the electronic record relates -
(i) if he is a body corporate or a registered partnership, his registered office; or
(ii) in any other case, his principal place of business.

(6) Where the originator or the addressee of an electronic record does not have a place of business, or the electronic record does not relate to the originator's business, the electronic record shall be deemed to have been sent or received -

(a) if it is a company, whether established in the Islands or in any other jurisdiction, at its registered office; or
(b) in any other case, at the place where he ordinarily resides.

Part V - Electronic Signatures

Equal treatment of signatures

18. Except as provided in section 19, this law shall not be applied so as to exclude, restrict or deprive of legal effect, any method of creating an electronic signature which -

(a) satisfies the requirements of section 19(1); or
(b) otherwise meets the requirements of an applicable statutory provision, rule of law, contract or deed.

Compliance with a requirement for a signature

19. (1) Where the signature of a person is required by a statutory provision, rule of law, contract or deed, that requirement shall be met in relation to an electronic record if an electronic signature is used that is as reliable as was appropriate for the purpose for which the electronic record was generated or communicated, in all the circumstances, including any relevant agreements.

(2) Subsection (1) applies whether the requirement for a signature is in the form of an obligation or the statutory provision, rule of law, contract or deed provides consequences for the absence of a signature.

(3) An electronic signature shall be reliable for the purpose of satisfying the requirement referred to in paragraph (1) if -

(a) the means of creating the electronic signature is, within the context in which it is used, linked to the signatory and to no other person;
(b) the means of creating the electronic signature was, at the time of signing, under the control of the signatory and of 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 integrity 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 any 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.

Determination of standards

20. The Governor may make regulations prescribing methods which satisfy the requirements of section 19.

Conduct of a person relying on an electronic signature

21. A person relying on an electronic signature shall bear the legal consequences of his failure to -

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

Recognition of foreign certificates and electronic signatures

22. (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.

(2) If the Minister, on the recommendation of the Authority, considers that the practices of a foreign information security service provider provide a level of reliability at least equivalent to that required of information security service providers in order that they may be approved under section 25, he may, by notice

published in the Gazette, recognise certificates or classes of certificates issued by the foreign provider as legally equivalent to certificates issued by information security service providers approved under section 25.

(3) The Minister may, by notice published in the Gazette, recognise signatures complying with the laws of a foreign jurisdiction relating to electronic signatures as legally equivalent to signatures issued by information security service providers approved under section 25 if the laws of the other foreign jurisdiction require a level of reliability at least equivalent to that required for such signatures under this Law.

(4) The Governor may make regulations prescribing the matters to be taken into account by the Minister when deciding whether to exercise his powers under subsections (2) and (3).

(5) Notwithstanding subsections (2) and (3), parties to commercial and other transactions may specify that a particular information security service provider, class of information security service providers or class of certificates shall be used in connection with messages or signatures submitted to them.

(6) Where, notwithstanding subsections (2) and (3), 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.

Notarisation and acknowledgment

23. Where information or a signature, document or record is required by a statutory provision, rule of law, contract or deed to be notarised, acknowledged, verified or made under oath, the requirement shall be satisfied if, in relation to an electronic signature, electronic document or electronic record, the electronic signature of the person authorised to perform those acts, together with all other information required to be included by other applicable law, is attached to or logically associated with the electronic signature, electronic document or electronic record.

Part VI - Information Security Service Providers

Register of approved providers

24. (1) The Minister may require the Authority to establish and maintain a register of approved information security services, and of providers of such services, which shall contain particulars of every person who, or service which, is for the time being approved under any arrangements in force under section 25.

(2) The Governor, on the recommendation of the Authority may make regulations prescribing the particulars that are to be included in entries in the register maintained under subsection (1).

(3) The Authority shall -

(a) allow public inspection, at all times, of an electronic copy of the register; and
(b) publicise any withdrawal or modification of an approval under section 25,

in accordance with arrangements prescribed by the Governor in regulations.

Arrangements for the grant of approvals

25. The Governor may make regulations enabling the Authority to grant approvals, whether subject to conditions or otherwise, on payment of a prescribed fee, to persons who -

(a) are providing information security services in the Islands or are proposing to do so; and
(b) seek approval in respect of any such services that they are providing, or are proposing to provide, whether in the Islands or elsewhere.

Restrictions on disclosure of information

26. (1) Subject to subsection (2), information which -

(a) has been obtained under or by virtue of this Part; and
(b) relates to the private affairs of any individual or to any particular business,

shall be deemed to be confidential information for the purposes of the Confidential Relationships (Preservation) Law (1995 Revision).

1995 Revision

(2) Section 5 of the Confidential Relationships (Preservation) Law (1995 Revision) does not apply to any disclosure of information which is made -

(a) for the purpose of facilitating the carrying out of any functions under this Part, or any prescribed functions, of the Minister or the Authority;
(b) for the purpose of facilitating the carrying out of prescribed functions of any prescribed person;
(c) in connection with the investigation by the police of a criminal offence or for the purposes of any criminal proceedings; or
(d) for the purposes of any civil proceedings which -
(i) relate to the provision of information security services; and
(ii) are proceedings to which a person approved in accordance with arrangements under section 24 is a party.

(3) If information is disclosed to the public in circumstances in which the disclosure does not contravene the Confidential Relationships (Preservation) Law (1995 Revision), that law shall not prevent its further disclosure by any person.

Provision of information security services.

27. (1) References in this Part to the provision of an information security service do not include references to the supply of, or of any right to use, computer software or computer hardware unless the supply or the right to use is integral to the provision of information security services which do not consist of such a supply or right to use.

(2) For the purposes of this Part, information security services are provided in the Islands if they are provided from premises in the Islands and -

(a) they are provided to a person who is in the Islands when he makes use of the services; or

(b) they are provided to a person who makes use of the services for the purposes of a business carried on in the Islands or from premises in the Islands.

Conduct of the information security service provider

28. (1) An information security service provider shall -

(a) act in accordance with the representations it makes with respect to its policies and practices;

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it -

(i) that are relevant to the certificate throughout its life cycle; or

(ii) which are included in the certificate;

(c) provide reasonably accessible means which enable a person who relies on the certificate to ascertain from the certificate -

(i) the identity of the information security service provider;

(ii) that the person who is identified in the certificate had control of the signature device at the time of signing;

(iii) that the signature device was operational on or before the date when the certificate was issued;

(d) provide reasonably accessible means which enable a person who relies on the certificate to ascertain, where relevant, from the certificate or otherwise -

(i) the method used to identify the signature device holder;

(ii) any limitation on the purpose or value for which the signature device or the certificate may be used;

(iii) that the signature device is operational and has not been compromised;

(iv) any limitation on the scope or extent of liability stipulated by the information security service provider;

(v) whether means exist for the signature device holder to give notice that a signature device has been compromised; and

(vi) whether a timely revocation service is offered;

(e) provide a means for a signature device holder to give notice that a signature device has been compromised and ensure the availability of a timely revocation service; and

(f) utilise trustworthy systems, procedures and human resources in performing its services.

(2) An information security service provider shall be liable for its failure to satisfy the requirements of subsection (1)

Criteria for determining trustworthiness

29. The Governor, on the recommendation of the Authority, may make regulations prescribing the factors to which regard shall be had in determining whether, and the extent to which, systems, procedures and human resources are trustworthy for the purposes of section 28(1)(f).

Contents of a certificate

30. The Governor, on the recommendation of the Authority, may make regulations prescribing the matters that shall be specified in a certificate.

Conduct of the signature device holder

31. A signature device holder shall -

(a) exercise reasonable care to avoid unauthorised use of its signature device;

(b) without undue delay, notify any person who may reasonably be expected by the signature device holder to rely on or to provide services in support of the electronic signature if -

(i) the signature device holder knows that the signature device has been compromised; or

(ii) the circumstances known to the signature device holder give rise to a substantial risk that the signature device may have been compromised; and

(c) where a certificate is used to support the electronic signature, exercise reasonable care to ensure the accuracy and completeness of all material representations made by the signature device holder, which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

Part VII - Intermediaries and E-commerce Service Providers

Liability of e-commerce service providers

32. (1) In proceedings against an intermediary or e-commerce service provider for a offence consisting of or arising out of the processing of an electronic record by means of his system, it shall be a defence for him to show that he was not the originator of the record and either -

(a) that he did not know, and had no reasonable cause to suspect that, the processing of the record would (apart from this subsection) constitute or give rise to that offence; or

(b) as soon as reasonably practicable after he knew or had reasonable cause to suspect that the processing of the record would (apart from this subsection) constitute or give rise to that offence that -

(i) he took such steps as were reasonable to prevent such processing by means of his system; and

(ii) he notified a constable of any relevant facts in his possession.

(2) An intermediary or e-commerce service provider shall not be subject to any civil liability in respect of an electronic record which is processed by means of his system if he was not the originator of the record and -

(a) he did not know and had no reasonable cause to suspect that the processing of it would (apart from this subsection) give rise to that liability; or

(b) as soon as reasonably practicable after he knew or had reasonable cause to suspect that the processing of the record would (apart from this subsection) give rise to that liability, he took such steps as were reasonable to prevent such processing by means of his system.

(3) An intermediary or e-commerce service provider shall not be subject to any civil liability for any action he takes in good faith under subsection (1)(b) or (2)(b).

(4) An intermediary or e-commerce service provider shall not be required to monitor any electronic record processed by means of his system in order to ascertain whether its processing would (apart from this section) constitute or give rise to an offence or give rise to civil liability.

(5) Except as provided by subsection (3), nothing in this section shall relieve an intermediary or e-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.

Part VIII - Data Protection

Data protection

33. (1) The Governor, on the recommendation of the Authority, may make regulations prescribing standards for the processing of personal data, whether or not the personal data originates inside the Islands.

(2) Regulations made under subsection (1) may provide for -

(a) the protection of privacy;
(b) the voluntary registration and de-registration to those standards by data controllers and data processors;
(c) the establishment by the Authority of a register that is available for public inspection showing particulars of data controllers and data processors who have registered or de-registered to those standards and the dates of such registration or de-registration, and the countries in respect of which the registration or de-registration applies;
(d) the application of those standards to the countries specified in the regulations;
(e) different standards to be applied in respect of personal data originating from different countries; and
(f) such matters as may be necessary or convenient for giving effect to this Part or for its administration.

(3) A data controller or data processor who voluntarily registers to a standard prescribed in regulations made under subsection (1) and who fails to comply with that standard, as it may be amended from time to time, in respect of 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 is guilty of an offence and liable on summary conviction to a fine of fifty thousand dollars and to imprisonment for six months, and if the offence of which he is convicted is continued after conviction he commits a further offence and liable to a fine of five thousand dollars for every day on which the offence is so continued.

Pseudonyms

34. (1) Information security service providers may, at the request of a particular signature device holder, indicate in the relevant certificate a pseudonym instead of the signature device holder's name.

(2) Where a pseudonym is indicated under subsection (1), the information security service provider shall, where necessary for the investigation by the police of an offence involving the use of electronic signatures, or where otherwise required by law to do so, transfer to a constable all personal data relating to the signature device holder that is in his possession.

(3) Where personal data is transferred under subsection (2), the information security service provider shall make a record of the transfer.

(4) The Governor may, by regulations, prescribe information that is to be provided in addition to the personal data that is to be transferred under subsection (2).

Part IX - Miscellaneous

Code of practice

35. (1) The Governor, on the recommendation of the Authority, may, by regulations, establish standards or conduct requirements with which e-commerce service providers or intermediaries carrying on business in or from within the Islands must comply.

(2) A standard established by regulations made under subsection (1) may relate to one or more of the following matters -

(a) the types of services that are permitted to be provided by intermediaries;
(b) the types of customers to whom services may be provided by intermediaries;
(c) the types of information permitted to be contained in an electronic record for which services are provided by intermediaries;
(d) the contractual application of relevant codes of conduct or standards to customers of intermediaries and e-commerce service providers;
(e) the information to be disclosed by intermediaries and e-commerce service providers including the name, address, e-mail address and contact and registration details;
(f) the actions to be taken in the event of customers of intermediaries or e-commerce service providers sending bulk, unsolicited electronic records;
(g) the practical application of the relevant laws of the Islands to intermediaries and e-commerce service providers;
(h) procedures for dealing with complaints;
(i) procedures for dispute resolution, including dispute resolution by electronic means; and
(j) such other matters as the Governor may require.

(3) Regulations made under subsection (1) shall provide -

(a) that an intermediary or e-commerce service provider who fails to comply with a standard prescribed in the regulations shall in the first instance be given a written warning by the Authority;
(b) that the Authority may direct that person to cease or correct his practices; and

(c) that if that person fails to do so within such period as may be stated in the direction, he commits an offence and is liable to such penalties as may be prescribed.

(4) If the Authority is satisfied that a person, body or organisation represents intermediaries or e-commerce service providers carrying on business in the Islands, the Authority may, by notice given to the person, body or organisation, request that person, body or organisation to -

(a) develop standards or conduct requirements that apply to intermediaries or e-commerce service providers and that deal with one or more specified matters relating to the provision of services by those intermediaries or e-commerce service providers; and
(b) provide details relating to those standards or conduct requirements to the Authority within such time as may be specified in the request.

(5) If the Minister, on the recommendation of the Authority, is satisfied with the standards and conduct requirements provided under subsection (4), he shall approve such standards and conduct requirements by notice published in the Gazette, and thereupon such standards and conduct requirements shall apply to such intermediaries or e-commerce service providers as may be specified in the notice.

(6) If the Minister has approved any standard or conduct requirement that applies to intermediaries or e-commerce service providers, and -

(a) he receives notice from a person, body or organisation representing intermediaries or e-commerce service providers or proposals to amend the standard or conduct requirement; or
(b) he no longer considers that the standard or conduct requirement is appropriate,

he may, by notice published in the Gazette, revoke or amend any existing standard or conduct requirement.

(7) References in this section to intermediaries and e-commerce service providers include references to a particular class of intermediaries or to a particular class of e-commerce service providers.

Offences by bodies corporate

36. (1) Where an offence under this Law, which has been committed by a body corporate, is proved to have been committed with the consent or connivance of, or to be attributable to any neglect on the part of, any director, manager, secretary or other similar officer of the body corporate, or any person who was

purporting to act in any such capacity, he, as well as the body corporate, is guilty of that offence and liable to be proceeded against and punished accordingly.

(2) Where the affairs of a body corporate are managed by its members, subsection (1) shall apply in relation to the acts and defaults of a member in connection with his functions of management as if he were a director of the body corporate.

Regulations

37. (1) Without derogating from the powers to make regulations conferred elsewhere in this Law, the Governor may make regulations -

(a) prescribing matters required or permitted by this Law to be prescribed;
(b) authorising or facilitating -
  (i) the investigation of; or
  (ii) the bringing of criminal proceedings in respect of the processing of electronic records that may be, or is, an offence under this or any other Law; or
(c) for carrying the purpose and provisions of this Law into effect.

(2) Regulations made under this Law may provide that the contravention of any provision constitutes an offence and may prescribe penalties for any such offence not exceeding the maximum fine and term of imprisonment prescribed in this Law for any offence under this Law.

Prohibition on key escrow requirements

38. (1) Nothing in this Law shall confer a power on the Governor, or a minister or official member or the Authority-

(a) by conditions of an approval under Part VI, or
(b) by any regulations under this Law,

to impose a requirement on any person to deposit a key for electronic records with another person.

(2) In this section -

"key", in relation to electronic records, means any code, password, algorithm or other data the use of which (with or without other keys) -

(a) allows access to the electronic record; or
(b) facilitates the putting of the electronic record into an intelligible form,

and references in this section to depositing a key for electronic records with a person include references to doing anything that has the effect of making the key available to that person.

Appointment of e-Business Advisory Board

39. (1) The Governor shall appoint a Board, to be known as the e-Business Advisory Board.

(2) The Board shall advise the Governor and the Minister -

(a) on the discharge of their functions under this Law;
(b) on any matter connected with the functions referred to in paragraph (a);
(c) on any matter connected with the administration of this Law; and
(d) on any matter referred to it by the Governor or the Minister that is connected or relates to the matters dealt with by this Law.

(3) The members of the Board shall hold office at the pleasure of the Governor.

(4) The Board shall consist of not less than seven nor more than ten persons appearing to the Governor to be knowledgeable about electronic business.

(5) The Board shall, at their first meeting, and at the first meeting in every calendar year thereafter, appoint one of their number to be the chairman of the Board until the date of the first meeting of the Board in the following calendar year.

(6) The Board shall determine its own procedure.

Publication in consolidated and revised form authorised by the Governor in Council this 10th day of June, 2003.

Carmena Watler
Clerk of Executive Council

(Price $ 5.60)