ELECTRONIC TRANSACTIONS ACT

(CHAPTER 88)

(Original Enactment: Act 16 of 2010)

REVISED EDITION 2011

(31st December 2011)

An Act to provide for the security and use of electronic transactions, to implement the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the United Nations on 23rd November 2005 and to provide for matters connected therewith.

[1st July 2010]

PART I
PRELIMINARY

Short title

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

Interpretation

2.

—(1) In this Act, unless the context otherwise requires —

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

"authorised officer", in relation to the exercise of any power or performance of any duty under this Act, means a person to whom the exercise of that power or performance of that duty has been delegated under section 27;

"automated message system" means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person each time an action is initiated or a response is generated by the program or electronic or other means;

"communication" includes any statement, declaration, demand, notice, request, offer or the acceptance of an offer, that the parties are required to make or choose to make in connection with the formation or performance of a contract;

"Controller" means the Controller appointed under section 27(1) and includes a Deputy or an Assistant Controller appointed under section 27(3);

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

"electronic communication" means any communication that the parties make by means of electronic records;

"electronic record" means a record generated, communicated, received or stored by electronic means in an information system or for transmission from one information system to another;

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

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

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

"public agency" means a department or ministry of the Government, an Organ of State or a public authority established by or under a public Act;

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

"rule of law" includes written law;

"secure electronic record" means an electronic record that is treated as a secure electronic record by virtue of section 17(1) or any other provision of this Act;

"secure electronic signature" means an electronic signature that is treated as a secure electronic signature by virtue of section 18 or any other provision of this Act;

"security procedure" means a procedure for the purpose of —

(*a*)

verifying that an electronic record is that of a specific person; or

(*b*)

detecting error or alteration in the communication, content or storage of an electronic record since a specific point in time,

which may require the use of algorithms or codes, identifying words or numbers, encryption, answerback or acknowledgment procedures, or similar security devices;

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

"specified security procedure" means a security procedure which is specified in the Second Schedule;

"specified security procedure provider" means a person involved in the provision of a specified security procedure.

(2) In this Act, "place of business", in relation to a party, means —

(*a*)

any place where the party maintains a non-transitory establishment to pursue an economic activity other than the temporary provision of goods or services out of a specific location; or

(*b*)

if the party is a natural person and he does not have a place of business, the person's habitual residence.

(3) For the purposes of subsection (2) —

(*a*)

if a party has indicated his place of business, the location indicated by him is presumed to be his place of business unless another party proves that the party making the indication does not have a place of business at that location;

(*b*)

if a party has not indicated a place of business and has more than one place of business, then the place of business is that which has the closest relationship to the relevant contract, having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract;

(*c*)

a location is not a place of business merely because that location is —

(i)

where equipment and technology supporting an information system used by a party in connection with the formation of a contract are located; or

(ii)

where the information system may be accessed by other parties; and

(*d*)

the sole fact that a party makes use of a domain name or an electronic mail address connected to a specific country does not create a presumption that its place of business is located in that country.

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

[ETA, ss. 2 and 18(4); UN, Art. 4, 6 and 9(3)(a); US, s. 106(2)]

Purposes and construction

3. This Act shall be construed consistently with what is commercially reasonable under the circumstances and to give effect to the following purposes:

(*a*)

to facilitate electronic communications by means of reliable electronic records;

(*b*)

to facilitate electronic commerce, to eliminate barriers to electronic commerce resulting from uncertainties over writing and signature requirements, and to promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;

(*c*)

to facilitate electronic filing of documents with public agencies, and to promote efficient delivery by public agencies of services by means of reliable electronic records;

(*d*)

to minimise the incidence of forged electronic records, intentional and unintentional alteration of records, and fraud in electronic commerce and other electronic transactions;

(*e*)

to help to establish uniformity of rules, regulations and standards regarding the authentication and integrity of electronic records;

(*f*)

to promote public confidence in the integrity and reliability of electronic records and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium; and

(*g*)

to implement the United Nations Convention on the Use of Electronic Communications in International Contracts adopted by the General Assembly of the United Nations on 23rd

November 2005 and to make the law of Singapore on electronic transactions, whether or not involving parties whose places of business are in different States, consistent with the provisions of that Convention.

[ETA, s. 3]

Excluded matters

4.

—(1) The provisions of this Act specified in the first column of the First Schedule shall not apply to any rule of law requiring writing or signatures in any of the matters specified in the second column of that Schedule.

(2) The Minister may, by order published in the *Gazette*, amend the First Schedule.

[ETA, s. 4]

Party autonomy

5.

—(1) Nothing in Part II shall affect any rule of law or obligation requiring the agreement or consent of the parties as to the form of a communication or record, and (unless otherwise agreed or provided by a rule of law) such agreement or consent may be inferred from the conduct of the parties.

(2) Nothing in Part II shall prevent the parties to a contract or transaction from —

(*a*)

excluding the use of electronic records, electronic communications or electronic signatures in the contract or transaction by agreement; or

(*b*)

imposing additional requirements as to the form or authentication of the contract or transaction by agreement.

(3) Subject to any other rights or obligations of the parties to a contract or transaction, the parties may, by agreement —

(*a*)

exclude section 6, 11, 12, 13, 14, 15 or 16 from applying to the contract or transaction; or

(*b*)

derogate from or vary the effect of all or any of those provisions in respect of the contract or transaction.

[ETA, s. 5; UN, Art. 3 and 8(2)]

PART II

ELECTRONIC RECORDS, SIGNATURES AND CONTRACTS

Legal recognition of electronic records

6. For the avoidance of doubt, it is declared that information shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic record.

[ETA, s. 6; UNCITRAL, Art. 5; UN, Art. 8]

Requirement for writing

7. Where a rule of law requires information to be written, in writing, to be presented in writing or provides for certain consequences if it is not, an electronic record satisfies that rule of law if the information contained therein is accessible so as to be usable for subsequent reference.

[ETA, s. 7; UNCITRAL, Art. 6; UN, Art. 9(2)]

Requirement for signature

8. Where a rule of law requires a signature, or provides for certain consequences if a document or a record is not signed, that requirement is satisfied in relation to an electronic record if —

(*a*)

a method is used to identify the person and to indicate that person's intention in respect of the information contained in the electronic record; and

(*b*)

the method used is either —

(i)

as reliable as appropriate for the purpose for which the electronic record was generated or communicated, in the light of all the circumstances, including any relevant agreement; or

(ii)

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

[UN, Art. 9(3)]

Retention of electronic records

9.

—(1) Where a rule of law requires any document, record or information to be retained, or provides for certain consequences if it is not, that requirement is satisfied by retaining the document, record or information in the form of an electronic record if the following conditions are satisfied:

(*a*)

the information contained therein remains accessible so as to be usable for subsequent reference;

(*b*)

the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received;

(*c*)

such information, if any, as 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; and

(*d*)

any additional requirements relating to the retention of such electronic records specified by the public agency which has supervision over the requirement for the retention of such records are complied with.

(2) An obligation to retain any document, record or information in accordance with subsection (1)(*c*) shall not extend to any information necessarily and automatically generated solely for the purpose of enabling a record 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 in paragraphs (*a*) to (*d*) of that subsection are complied with.

(4) Nothing in this section shall apply to —

(*a*)

any rule of law which expressly provides for the retention of documents, records or information in the form of electronic records; or

(*b*)

any rule of law requiring that any document, record or information be retained (or which provides for consequences if not) that the Minister, by order published in the *Gazette*, excludes from the application of this section in respect of such document, record or information.

[ETA, s. 9; UNCITRAL, Art. 10]

Provision of originals

10.

—(1) Where a rule of law requires any document, record or information to be provided or retained in its original form, or provides for certain consequences if it is not, that requirement is satisfied by providing or retaining the document, record or information in the form of an electronic record if the following conditions are satisfied:

(*a*)

there exists a reliable assurance as to the integrity of the information contained in the electronic record from the time the document, record or information was first made in its final form, whether as a document in writing or as an electronic record;

(*b*)

where the document, record or information is to be provided to a person, the electronic record that is provided to the person is capable of being displayed to the person; and

(*c*)

any additional requirements relating to the provision or retention of such electronic records specified by the public agency which has supervision over the requirement for the provision or retention of such records are complied with.

(2) For the purposes of subsection (1)(*a*) —

(*a*)

the criterion for assessing integrity shall be whether the information has remained complete and unaltered, apart from the introduction of any changes that arise in the normal course of communication, storage and display; and

(*b*)

the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(3) A person may satisfy the requirement referred to in subsection (1) by using the services of any other person, if the conditions in paragraphs (*a*), (*b*) and (*c*) of that subsection are complied with.

(4) Nothing in this section shall apply to any rule of law requiring that any document, record or information be provided or retained in its original form (or which provides for consequences if not) that the Minister, by order published in the *Gazette*, excludes from the application of this section in respect of such document, record or information.

[UNCITRAL, Art. 8; UN, Art. 9(4) and (5)]

Formation and validity of contracts

11.

—(1) For the avoidance of doubt, it is declared that in the context of the formation of contracts, an offer and the acceptance of an offer may be expressed by means of electronic communications.

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

[ETA, s. 11; UNCITRAL, Art. 11(1); UN, Art. 8(1)]

Effectiveness between parties

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

[ETA, s. 12; UNCITRAL, Art. 12(1)]

Time and place of despatch and receipt

13.

—(1) The time of despatch of an electronic communication is —

(*a*)

the time when it leaves an information system under the control of the originator or of the party who sent it on behalf of the originator; or

(*b*)

if the electronic communication has not left an information system under the control of the originator or of the party who sent it on behalf of the originator, the time when the electronic communication is received.

(2) The time of receipt of an electronic communication is the time when the electronic communication becomes capable of being retrieved by the addressee at an electronic address designated by the addressee.

(3) The time of receipt of an electronic communication at an electronic address that has not been designated by the addressee is the time when the electronic communication becomes capable of being retrieved by the addressee at that address and the addressee becomes aware that the electronic communication has been sent to that address.

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

(5) An electronic communication is deemed to be despatched at the place where the originator has its place of business and is deemed to be received at the place where the addressee has its place of business.

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

[ETA, s. 15; UN, Art. 10]

Invitation to make offer

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

[UN, Art. 11]

Use of automated message systems for contract formation

15. A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied validity or enforceability solely on the ground that no natural person reviewed or intervened in each of the individual actions carried out by the automated message systems or the resulting contract.

[UN, Art. 12]

Error in electronic communications

16.

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

(2) Subsection (1) shall not apply unless the person, or the party on whose behalf that person was acting —

(*a*)

notifies the other party of the error as soon as possible after having learned of the error and indicates that he made an error in the electronic communication; and

(*b*)

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

(3) Nothing in this section shall affect the application of any rule of law that may govern the consequences of any error other than as provided for in subsections (1) and (2).

[UN, Art. 14]

PART III

SECURE ELECTRONIC RECORDS AND SIGNATURES

Secure electronic record

17.

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

(2) For the purposes of this section and section 18, whether a security procedure is commercially reasonable shall be determined having regard to the purposes of the procedure and the commercial circumstances at the time the procedure was used, including —

(*a*) the nature of the transaction;

(*b*) the sophistication of the parties;

(*c*) the volume of similar transactions engaged in by either or all parties;

(*d*) the availability of alternatives offered to but rejected by any party;

(*e*) the cost of alternative procedures; and

(*f*) the procedures in general use for similar types of transactions.

[ETA, s. 16]

Secure electronic signature

18.

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

(*a*) unique to the person using it;

(*b*) capable of identifying such person;

(*c*) created in a manner or using a means under the sole control of the person using it; and

(*d*) linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated, such signature shall be treated as a secure electronic signature

.

(2) Whether a security procedure is commercially reasonable shall be determined in accordance with section 17(2).

[ETA, s. 17]

Presumptions relating to secure electronic records and signatures

19.

—(1) In any proceedings involving a secure electronic record, it shall be presumed, unless evidence to the contrary is adduced, that the secure electronic record has not been altered since the specific point in time to which the secure status relates.

(2) In any proceedings involving a secure electronic signature, it shall be presumed, unless evidence to the contrary is adduced, that —

(*a*) the secure electronic signature is the signature of the person to whom it correlates; and

(*b*) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

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

[ETA, s. 18]

PART IV

REGULATION OF SPECIFIED SECURITY PROCEDURES AND SPECIFIED SECURITY PROCEDURE PROVIDERS

Interpretation of this Part

20.

—(1) In this Part, "designated person" means any member of a class of specified security procedure providers specified in the Fourth Schedule.

(2) For the avoidance of doubt, a reference to this Part shall include a reference to the Second, Third and Fourth Schedules.

Specified security procedures

21.

—(1) The Minister may, by order published in the *Gazette*, amend the Second Schedule to add, delete or modify any specified security procedure for the purposes of this Act.

(2) The provisions set out in the Third Schedule shall apply to the corresponding specified security procedures.

(3) The Minister may, by order published in the *Gazette*, amend the Third Schedule to make provisions relating to any of the specified security procedures, including —

(*a*) specifying the conditions under which any electronic signature may be treated as a secure electronic signature;

(*b*) specifying the conditions under which any electronic record may be treated as a secure electronic record;

(*c*) prescribing the effect of and duties relating to the use of specified security procedures, including the rights and duties of any persons relating to the use of such procedures and specifying rules relating to the presumptions, assumption of risk, foreseeability of reliance and liability limits applicable to the use of specified security procedures; and

(*d*) prescribing offences in respect of the contravention of any provision in that Schedule, and prescribing fines not exceeding $20,000 or imprisonment which may not exceed 2 years or both, that may, on conviction, be imposed in respect of any such offence.

(4) The Minister may, by order published in the *Gazette*, amend the Fourth Schedule.

Regulation of specified security procedures and specified security procedure providers

22.

—(1) The Minister may make regulations for the carrying out of this Part and, without prejudice to such general power, may make regulations for all or any of the following purposes:

(*a*) the regulation, licensing or accreditation of specified security procedure providers and their authorised representatives;

(*b*) safeguarding or maintaining the effectiveness and efficiency of the common security infrastructure relating to the use of secure electronic signatures and the authentication of electronic records, including the imposition of requirements to ensure interoperability between specified security procedure providers or in relation to any security procedure;

(*c*) ensuring that the common security infrastructure relating to the use of secure electronic signatures and the authentication of electronic records complies with Singapore's international obligations;

(*d*) prescribing the forms and fees applicable for the purposes of this Part.

(2) Without prejudice to the generality of subsection (1), the Minister may, in making regulations for the regulation, licensing or accreditation of specified security procedure providers and their authorised representatives —

(*a*) prescribe the accounts to be kept by specified security procedure providers;

(*b*) provide for the appointment and remuneration of an auditor, and for the costs of an audit carried out under the regulations;

(*c*) provide for the establishment and regulation of any electronic system by a specified security procedure provider, whether by itself or in conjunction with other specified security procedure providers, and for the imposition and variation of requirements or conditions relating thereto as the Controller may think fit;

(*d*) make provisions to ensure the quality of repositories and the services they provide, including provisions for the standards, licensing or accreditation of repositories;

(*e*) provide for the use of any accreditation mark in relation to the activities of specified security procedure providers and for controls over the use thereof;

(*f*) prescribe the duties and liabilities of specified security procedure providers registered, licensed or accredited under this Act in respect of their customers; and

(*g*) provide for the conduct of any inquiry into the conduct of specified security procedure providers and their authorised representatives and the recovery of the costs and expenses involved in such an inquiry.

(3) Without prejudice to the generality of subsection (1), the Minister may make regulations to provide for the cross-border recognition of specified security procedure providers or specified security procedures or any processes or records related thereto, including any requirements —

(*a*) relating to interoperability arrangements with the specified security procedure providers;

(*b*) whether the specified security procedure providers satisfy certain requirements applicable to specified security procedure providers registered, accredited or licensed under this Act;

(*c*) whether the specified security procedures, processes or records satisfy certain requirements applicable to specified security procedures, processes or records (as the case may be) under this Act;

(*d*) that the processes or records have been guaranteed by a specified security procedure provider registered, accredited or licensed under this Act;

(*e*) that —

(i) the specified security procedure providers have been registered, accredited or licensed;

(ii) the processes have been specified; or

(iii) the records have been registered, under a particular registration, accreditation or licensing scheme (as the case may be) established outside Singapore; or

(*f*) that the specified security procedure providers, specified security procedures, processes or records have been recognised under a particular bilateral or multilateral agreement with Singapore.

(4) Regulations made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties for a fine not exceeding $50,000 or imprisonment for a term not exceeding 12 months or both.

[ETA, ss. 42, 43 and 46]

Controller may give directions for compliance

23.

—(1) The Controller may, by notice in writing, direct any designated person, or any officer, employee or authorised representative of a designated person —

(*a*) to take such measures or stop carrying on such activities as are specified in the notice if they are necessary to ensure compliance with this Part; or

(*b*) to co-operate with any other designated persons or public agencies as the Controller thinks necessary in the case of a public emergency.

(2) Any person who fails to comply with any direction specified in a notice issued under subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 12 months or to both.

(3) If any doubt arises as to the existence of a public emergency for the purposes of subsection (1)(*b*), a certificate signed by the Minister delivered to the designated person shall be conclusive evidence of the matters stated therein.

[ETA, s. 51]

Power to investigate

24.

—(1) The Controller or an authorised officer may investigate the activities of any designated person, or any officer, employee or authorised representative of a designated person, in relation to their compliance with this Part.

(2) For the purposes of subsection (1), the Controller may in writing issue an order to any designated person, or any officer, employee or authorised representative of a designated person, to further an investigation under this section or to secure compliance with this Part, including an order to produce records, accounts, data and documents kept by the designated person, and to allow the Controller or an authorised officer to examine and copy any of them.

[ETA, ss. 52 and 55(a)]

PART V

USE OF ELECTRONIC RECORDS AND SIGNATURES BY PUBLIC AGENCIES

Acceptance of electronic filing and issue of documents

25.

—(1) Any public agency that, pursuant to any written law —

(*a*) accepts the filing of documents, or obtains information in any form;

(*b*) requires that documents be created or retained;

(*c*) requires documents, records or information to be provided or retained in their original form;

(*d*) issues any permit, licence or approval; or

(*e*) requires payment of any fee, charge or other amount by any method and manner of payment,

may, notwithstanding anything to the contrary in such written law, carry out that function by means of electronic records or in electronic form.

(2) In any case where a public agency decides to perform any of the functions in subsection (1) by means of electronic records or in electronic form, the public agency may specify —

(*a*) the manner and format in which such electronic records shall be filed, created, retained, issued or provided;

(*b*) where such electronic records have to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a particular type of secure electronic signature);

(*c*) the manner and format in which such signature shall be affixed to the electronic record, and the identity of or criteria that shall be met by any specified security procedure provider used by the person filing the document;

(*d*) such control processes and procedures as may be appropriate to ensure adequate integrity, security and confidentiality of electronic records or payments; and

(*e*) any other required attributes for electronic records or payments that are currently specified for corresponding paper documents.

(3) For the avoidance of doubt, notwithstanding anything to the contrary in any written law but subject to any specification made under subsection (2), where any person is required by any written law to —

(*a*) file any document with or provide information in any form to a public agency;

(*b*) create or retain any document for a public agency;

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

(*d*) provide to or retain for a public agency any document, record or information in its original form; or

(*e*) hold a licence, permit or other approval from a public agency, such a requirement is satisfied by an electronic record specified by the public agency for that purpose and —

(i) in the case of a requirement referred to in paragraph (*a*), (*c*) or (*d*), transmitted or retained (as the case may be) in the manner specified by the public agency;

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

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

(4) Subject to sections 9 and 10, nothing in this Act shall by itself compel any public agency to accept or issue any document or information in the form of electronic records or to accept any payment in electronic form.

[ETA, s. 47]

PART VI
LIABILITY OF NETWORK SERVICE PROVIDERS

Liability of network service providers

26.

—(1) Subject to subsection (2), a network service provider shall not be subject to any civil or criminal liability under any rule of law in respect of third-party material in the form of electronic records to which he merely provides access if such liability is founded on —

(*a*) the making, publication, dissemination or distribution of such materials or any statement made in such material; or

(*b*) the infringement of any rights subsisting in or in relation to such material.

(2) Nothing in this section shall affect —

(*a*) any obligation founded on contract;

(*b*) the obligation of a network service provider as such under a licensing or other regulatory regime established under any written law;

(*c*) any obligation imposed under any written law or by a court to remove, block or deny access to any material; or

(*d*) any liability of a network service provider under the Copyright Act (Cap. 63) in respect of —

(i) the infringement of copyright in any work or other subject-matter in which copyright subsists; or

(ii) the unauthorised use of any performance, the protection period of which has not expired.

(3) In this section —

"performance" and "protection period" have the same meanings as in Part XII of the Copyright Act;

"provides access", in relation to third-party material, means the provision of the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access;

"third-party", in relation to a network service provider, means a person over whom the provider has no effective control.

[ETA, s. 10]

PART VII
GENERAL

Appointment of Controller and other officers

27.

—(1) The Minister may appoint any person to be the Controller for the purposes of this Act.

(2) The Controller shall, subject to any general or special directions of the Minister, perform such duties as are imposed and may exercise such powers as are conferred upon him by this Act or any other written law.

(3) The Controller may, after consultation with the Minister, appoint by name or office such number of Deputy Controllers, Assistant Controllers and other officers as the Controller considers necessary for the purpose of assisting him in the performance of his duties and the exercise of his powers under this Act.

(4) The Controller may delegate the exercise of all or any of the powers conferred or duties imposed upon him by this Act (except the power of delegation conferred by this subsection) to any officer appointed under subsection (3), subject to such conditions or limitations as the Controller may specify.

(5) In exercising any of the powers of enforcement under this Act, an authorised officer shall on demand produce to the person against whom he is acting the authority issued to him by the Controller.

(6) The Controller, every officer appointed under subsection (3) and every authorised officer shall be deemed to be a public servant for the purposes of the Penal Code (Cap. 224).

[ETA, ss. 41 and 50]

Obligation of confidentiality

28.

—(1) No person shall disclose any information which has been obtained by him in the performance of his duties or the exercise of his powers under this Act, unless such disclosure is made —

(*a*) with the permission of the person from whom the information was obtained or, where the information is the confidential information of a third person, with the permission of the third person;

(*b*) for the purpose of the administration or enforcement of this Act;

(*c*) for the purpose of assisting any public officer or officer of any other statutory board in the investigation or prosecution of any offence under any written law; or

(*d*)

in compliance with the requirement of any court or the provisions of any written law.

(2) For the purposes of this section, the reference to a person disclosing any information includes his permitting any other person to have access to any electronic record, book, register, correspondence, information, document or other material which has been obtained by him in the performance of his duties or the exercise of his powers under this Act.

(3) Any person who contravenes subsection (1) shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both.

[ETA, s. 48; ACRA, s. 34]

Access to computers and data

29.

—(1) The Controller or an authorised officer shall be entitled at any time to —

(*a*) have access to and inspect and check the operation of any computer system and any associated apparatus or material which he has reasonable cause to suspect is or has been in use in connection with any offence under this Act; and

(*b*) use or caused to be used any such computer system to search any data contained in or available to such computer system.

(2) The Controller or an authorised officer shall be entitled to require —

(*a*) the person by whom or on whose behalf the Controller or authorised officer has reasonable cause to suspect the computer is or has been so used; or

(*b*) any person having charge of, or otherwise concerned with the operation of, the computer, apparatus or material, to provide him with such reasonable technical and other assistance as he may require for the purposes of subsection (1).

(3) Any person who —

(*a*) obstructs the lawful exercise of the powers under subsection (1); or

(*b*) fails to comply with a request under subsection (2), shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 12 months or to both.

[ETA, s. 53]

Production of documents, etc.

30. The Controller or an authorised officer shall, for the purposes of the execution of this Act, have power to do all or any of the following:

(*a*) require the production of any identification document from any person in relation to any offence under this Act;

(*b*) make such inquiry as may be necessary to ascertain whether the provisions of this Act have been complied with.

[ETA, s. 55]

Obstruction of Controller or authorised officer

31. Any person who obstructs, impedes, assaults or interferes with the Controller or any authorised officer in the performance of his functions under this Act shall be guilty of an offence.

[ETA, s. 54]

Offences by bodies corporate, etc.

32.

—(1) Where an offence under this Act committed by a body corporate is proved —

(*a*) to have been committed with the consent or connivance of an officer; or

(*b*) to be attributable to any neglect on his part, the officer as well as the body corporate shall be guilty of the offence and shall be 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.

(3) Where an offence under this Act committed by a partnership is proved —

(*a*) to have been committed with the consent or connivance of a partner; or

(*b*) to be attributable to any neglect on his part, the partner as well as the partnership shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(4) Where an offence under this Act committed by an unincorporated association (other than a partnership) is proved —

(*a*) to have been committed with the consent or connivance of an officer of the unincorporated association or a member of its governing body; or

(*b*) to be attributable to any neglect on the part of such an officer or member, the officer or member as well as the unincorporated association shall be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(5) In this section —

"body corporate" includes a limited liability partnership;

"officer" —

(*a*) in relation to a body corporate, means any director, partner, member of the committee of management, chief executive, manager, secretary or other similar officer of the body corporate and includes any person purporting to act in any such capacity; or

(*b*) in relation to an unincorporated association (other than a partnership), means the president, the secretary, or any member of the committee of the unincorporated association, or any person holding a position analogous to that of president, secretary or member of such a committee and includes any person purporting to act in any such capacity;

"partner" includes a person purporting to act as a partner.

(6) Regulations may provide for the application of any provision of this section, with such modifications as the Minister considers appropriate, to any body corporate or unincorporated association formed or recognised under the law of a territory outside Singapore.

[ETA, s. 49]

General penalties

33. Any person guilty of an offence under this Act for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 6 months or to both.

[ETA, s. 56]

Consent of Public Prosecutor

34. No prosecution in respect of any offence under this Act shall be instituted except by or with the consent of the Public Prosecutor.

[ETA, s. 57]

Jurisdiction of court

35. Notwithstanding any provision to the contrary in the Criminal Procedure Code 2010 (Act 15 of 2010), a District Court shall have jurisdiction to try any offence under this Act and shall have power to impose the full penalty or punishment in respect of the offence.

[ETA, s. 58]

Composition of offences

36.

—(1) The Controller may, in his discretion, compound any offence under this Act which is prescribed as being an offence which may be compounded by collecting from the person reasonably suspected of having committed the offence a sum not exceeding —

(*a*) one half of the amount of the maximum fine that is prescribed for the offence; or

(*b*) $5,000,

whichever is the lower.

(2) On payment of such sum of money, no further proceedings shall be taken against that person in respect of the offence.

(3) The Minister may make regulations prescribing the offences which may be compounded.

[ETA, s. 59]

Power to exempt

37. The Minister may, by order published in the *Gazette*, exempt, subject to such terms and conditions as he thinks fit, any person or class of persons from all or any of the provisions of this Act.

[ETA, s. 60]

Regulations

38. The Minister may make regulations to prescribe anything which is required to be prescribed under this Act (except section 22) and generally for the carrying out of the provisions of this Act (except section 22).

[ETA, s. 61]

Transitional provisions

39.

—(1) Subject to subsection (2), this Act shall apply to all acts or transactions done in relation to an electronic record, including the generation, signing or communication of an electronic record, made on or after the date of commencement of this Act.

(2) If, immediately before the date of commencement of this Act —

(*a*) by virtue of section 8 of the repealed Electronic Transactions Act (Cap. 88, 1999 Ed.) (referred to in this section as the repealed Act), an electronic signature was treated as having satisfied a rule of law requiring a signature, or providing certain consequences if a document is not signed;

(*b*) by virtue of section 9 of the repealed Act, an electronic record was treated as having satisfied a rule of law requiring certain documents, records or information to be retained; or

(*c*) by virtue of section 15 of the repealed Act, an electronic record was treated as having been despatched or received,

the provisions of this Act shall not affect that treatment of the electronic signature or electronic record, as the case may be.