Draft
I.S.M/L.P.
12.03.12
11.06.12
18.06.12
24.08.12
07.09.12
10.09.12
05.10.12
16.10.12
04.12.12
12.12.12
23.04.13
06.06.13
03.07.13

Bill No. of 2013

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS BILL, 2013
(Published on , 2013)

MEMORANDUM

1. A draft of the above Bill, which is intended to be presented to the National Assembly, is set out below.

2. The object of the Bill is to –

(a) facilitate the use of electronic means of communication so as to enable –

(i) legal recognition and validity of electronic commercial transactions conducted internally and externally,

(ii) recognition, promotion and implementation of information technologies which facilitate electronic commerce,

(iii) electronic transactions to be recognised in the same manner as paper based transactions,

(iv) the promotion of a legal framework to support electronic commercial practices, and

(v) the promotion and adoption of information technologies in relation to electronic transactions;

(b) give electronic signatures the legal equivalence to the handwritten signature;

(c) promote a technology-neutral legal framework for the creation of e-signatures;

(d) give legal recognition to certificates created or issued locally or externally;

(e) provide functional equivalence of electronic information to written information such that certain legal requirements for information retention, presentation of information or information admissible as evidence is recognised regardless of form; and

(f) promote uniformity of legislation and support commercial practices with legal coverage.

3. Part II of the Bill provides for the legal recognition of electronic communications while Part III provides for the legality of electronic transactions. Part IV provides for the transmission of electronic communications, Part V provides for secure electronic signatures. Part VI provides for consumer protection while Part VII provides for on-line marketing. Part VIII of the Bill provides for the liability of service providers while Part IX provides for general provisions like offences, penalties and the power to make regulations.

....
KELETSO J. RAKHUDU
Acting Minister for Trade and Industry

ARRANGEMENT OF SECTIONS

A BILL
-entitled-

An Act to provide for the facilitation and regulation of electronic communications and transactions; to provide specifically for electronic commerce and electronic signatures and for matters incidental and connected thereto.

Date of Assent:
Date of Commencement:
ENACTED by the Parliament of Botswana

PART I - *Preliminary*

Short title and commencement

1. This Act may be cited as the Electronic Communications and Transactions Act, 2013 and shall come into operation on such a date as the Minister may, by Order published in the *Gazette*, appoint.

Interpretation

2. 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 in respect of that electronic communication;

"automated message system" means a pre-programmed, or other automated system used to initiate an action, respond to electronic communications, or to generate other performances in whole or in part, without review or intervention by a person each time an action is initiated or a response is generated by the system;

"cache" means high speed memory that stores data for relatively short periods of time in information systems in order to speed up data transmission or processing;

"certificate" means an electronic attestation which links signature verification data to a person and confirms the identity of the person;

"certification service provider' means a person providing an authentication product or service incorporated in or logically associated with an electronic communication;

"Communications Regulatory Authority" means the Communications Regulatory Authority established under section 3 of the Communications Regulatory Authority Act;

Act No.19 of 2012

"consumer" means an individual who enters or intends to enter into an electronic transaction with a supplier for the supply of goods or services offered by that supplier;

"data message" means information generated, sent, received, or stored by electronic, magnetic, optical or similar means, including but not limited to, electronic data interchange, electronic mail, mobile communications, such as short message service (SMS) messages, and audio or video recordings;

"direct costs" means costs incurred in the return of the goods or services such as transport costs or postage but excludes any handling fees;

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

"electronic communication" means information generated, communicated, processed, sent, received, recorded, stored or displayed by electronic means;

"electronic data interchange" means the electronic transfer of structured data from one information system to another information system in accordance with agreed standards;

"electronic record" means data that is recorded or stored on any medium in or by a computer system or other similar device and that can be read or perceived by a person or a computer system or other similar device, and includes a display, print out or other output of that data;

"electronic signature" means data in electronic form attached to or logically subjoined to an electronic communication, and which can be used to identify the signatory (method of authentication) and indicate consent for the information contained in the said communication;

"electronic transaction" means a transaction, action or set of actions of either a commercial or non-commercial nature, and includes the provision of information or e-government services;

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

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

"information system services" means providing the connection and network facilities necessary for the transmission, hosting and routing of electronic communications between or among points specified by a user of data of the user's choosing, without modification to the content of the data sent, stored or received;

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

"secure electronic signature" means a signature duly recognised as such in terms of Part V; and

"service provider" means a person or party that makes information system services available.

PART II – *Legal recognition of Electronic Communications*

Legal recognition of electronic communications

3. Subject to the provisions of this Act, information shall not be denied legal effect, validity or enforcement solely on the grounds that –

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

(b) it is not contained in the electronic communication purporting to give rise to such legal effect, but is merely referred to in that electronic communication.

Information required in writing

4.(1) Where in any law, a person is required to or permitted to give information in writing, that requirement or permission is met if the information is given in the form of an electronic communication that is accessible for use in any subsequent reference.

(2) Subsection (1) shall apply irrespective of whether –

(a) the requirement is an obligation; or

(b) the law which requires the giving of such information also provides consequences for the information not being in writing.

Legal recognition of electronic signatures

5. Subject to the provisions of this Act, an electronic signature shall not be denied legal effect, validity or enforcement solely on the grounds that it is in electronic form.

Signatures

6.(1) Subject to Part V of this Act, where any law requires the signature of a person, that requirement is met if the signature is given in relation to an electronic communication or transaction and there is a method –

(a) which is used to identify that person and to indicate that person's approval of the information contained in the electronic communication or transaction; or

(b) which, having regard to all the relevant circumstances, is as reliable as was appropriate for the purpose for which the electronic communication or transaction was generated or communicated.

(2) Subsection (1) shall apply irrespective of whether –

(a) the requirement is an obligation; or

(b) the law which requires the signature also provides consequences for the absence of a signature.

Requirement for originals

7.(1) Where in any law, a person is required to present or retain information in its original form, that requirement shall be satisfied by an electronic communication if –

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as an electronic communication or otherwise as an assessment under subsection (2) may establish; and

(b) that information is capable of being displayed to the person to whom it is to be presented.

(2) For purposes of subsection (1)*(a)* –

(a) the criteria for assessing the integrity of information shall be 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 shall be assessed in the light of the purpose for which the information was generated and in light of all the relevant circumstances.

(3) Subsection (1) shall apply irrespective of whether –

(a) the requirement is an obligation; or

(b) the law which imposes the requirement also provides consequences for non-compliance.

Admissibility and evidential weight of electronic communications

8.(1) Subject to the Electronic Evidence Act, in any legal proceedings, the rules of evidence shall not be applied so as to deny the admissibility of an electronic communication in evidence -

(a) solely on the ground that it is an electronic communication; or

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2) Information in the form of an electronic communication shall be given due evidential weight.

(3) In assessing the evidential weight of an electronic communication, regard shall be had to –

(a) the reliability of the manner in which the data message was generated, stored or communicated;

(b) the reliability of the manner in which the integrity of the electronic communication was maintained;

(c) the manner in which the originator of the data message was identified; and

(d) any other relevant circumstances.

Requirement for retention of information

9.(1) Where in any law, a person is required to retain certain documents, records or information, that requirement is satisfied by retaining an electronic communication, if –

(a) the information contained in the electronic communication is accessible so as to be usable for subsequent reference;

(b) the electronic communication is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) the origin and destination of the electronic communication and the date and time when it was sent or received can be determined.

(2) An obligation to retain any document, record or information under 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 of subsection (1) by using the services of any other person, provided that the conditions set forth in subsection (1) are met.

(4) Subsection (1) shall apply irrespective of whether –

(a) the requirement for retention of information is

an obligation; or

(b) the law which imposes the requirement for retention of information also provides consequences for non-compliance.

Requirement for production of document or information

10.(1) Where in any law, a person is required to produce a document or information, that requirement is met if the person produces, by means of an electronic communication, an electronic form of that document or information, and if -

(a) considering all the relevant circumstances at the time that the electronic communication was sent, the method of generating the electronic form of that document provided a reliable means of ensuring the maintenance of the integrity of the information contained in that document; and

(b) at the time the electronic communication was sent, it was reasonable to expect that the information contained in the communication would be readily accessible so as to be usable for subsequent reference.

(2) For purposes of subsection (1) the criteria for assessing the integrity of the information contained in the document shall be whether the information has remained complete and unaltered, except for -

(a) the addition of any endorsement; or

(b) any change which arises in the normal course of communication, storage and display;

Notarisation and certification

11.(1) Where a law requires a signature, statement or document to be notarised or verified, that requirement is met if the secure electronic signature of the person authorised to notarise or verify is attached to, incorporated in or logically associated with the electronic signature or electronic communication.

(2) Where a law requires or permits a person to provide a certified copy of a document and the document exists in electronic form, that requirement is met if the person provides a print-out certified to be a true reproduction of the document or information.

(3) Where a law requires or permits a person to provide a

certified copy of a document and the document exists in paper or other physical form, that requirement is met if an electronic copy of the document is certified to be a true copy and the certification is confirmed by the use of a secure electronic signature.

PART III - *Legality of Electronic Transactions*

Variation by agreement

12. As between parties involved in generating, sending, receiving, storing or otherwise processing electronic communications, and except as otherwise provided, the provisions of this Part may be varied by agreement.

Formation and validity of contracts

13.(1) Subject to subsection (2) and unless otherwise agreed to by the parties, an offer and the acceptance of an offer may be expressed by means of an electronic communication.

(2) A contract shall not be denied legal effect, validity or enforceability on the sole ground that an electronic communication was used wholly or partly in the formation of the contract.

(3) A proposal to conclude a contract made through one or more electronic communications which is not addressed to one or more specific parties, but is generally accessible to parties making use of information systems, including proposals that make use of interactive applications for the placement of orders through such information systems, shall 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.

Recognition of electronic communication by parties

14. 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.

Use of electronic signatures by parties

15. Subject to Part V, where two parties agree to make use of electronic signatures, they may agree to use any method of signing that they may deem appropriate.

Time of contract formation

16.(1) Where parties conclude a contract through an electronic communication such contract is deemed to be formed at the time when and the place where the acceptance of the offer becomes effective.

(2) An offer in the form of an electronic communication becomes effective at the time it is received by the offeree.

(3) The acceptance of an offer by means of an electronic communication becomes effective at the time and place that the electronic communication is received by the offeror.

Use of automated message system for contract formation

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

Error in electronic communications

18.(1) Where a natural person makes an input error in an electronic communication exchanged with an 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 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 learnt of the error and indicates that he or she made an error in the electronic communication and wishes to cancel the contract or cancel the input error;

(b) takes reasonable steps, including steps that conform to the other party's instructions, to return the goods or services received, if any, as a result of the error or, if instructed to do so, to destroy the goods or services, or to cancel the input error; and

(c) has not used or received any material benefit or value from the goods or services, or the input error, if any, from the other party.

(3) If a person has paid for any goods or services prior to exercising a right referred to in subsection (1), such person is entitled to a full refund of payment, which refund shall be made within 30 days from the date of cancellation.

Exclusions

19. The provisions of this Part shall not apply to the following -

(a) the creation or execution of a will;

(b) the creation, performance or enforcement of an indenture, declaration of trust or power of attorney;

(c) any contract for the sale or disposition of immovable property, or the sale or disposition of any interest in such property; and

(d) the transfer or conveyance of any immovable property or the transfer or conveyance of interest in such property.

PART IV – *Transmission of Electronic Communications*

Attribution of electronic communications

20.(1) An electronic communication is that of the originator if it was sent by –

(a) the originator personally;

(b) a person who had the authority to act on behalf of the originator in respect of that electronic communication; or

(c) an information system programmed by, or on behalf of the originator to operate automatically unless it can be proved that the information system did not properly execute such programming.

(2) As between the originator and the addressee of an electronic communication, an addressee is entitled to regard an electronic communication as being that of the originator, if -

(a) in ascertaining whether the electronic communication is that of the originator, the addressee properly applies a procedure previously agreed to by the originator for that purpose; or

(b) the electronic communication 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 the electronic communication as its own.

(3) Subsection (2) shall not apply –

(a) where the addressee receives notice from the originator that the electronic communication is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within subsection (2)(*b*), where the addressee knew or should have known, had he or she exercised reasonable care or used any agreed procedure, that the electronic communication was not that of the originator.

(4) An addressee is entitled to regard an electronic communication he or she receives as being what the originator intended to send and to act on that assumption except that the addressee shall not regard an electronic communication he or she receives to be that of the originator where, upon exercising reasonable care or using any agreed procedure the addressee knew or should have known that the electronic communication as received was erroneously transmitted.

(5) An addressee is entitled to regard each electronic communication he or she receives as being a separate electronic communication and to act on that assumption except that the addressee shall not regard as separate, an electronic communication that duplicates another electronic communication where, upon exercising reasonable care or using any agreed procedure the addressee knew or should have known that the electronic communication was a duplicate.

Time of dispatch of electronic communications

21.(1) The dispatch of an electronic communication occurs when it enters an information system outside the control of the originator or of the person who sent the electronic communication on behalf of the originator.

(2) Where the originator and the addressee are in the same information system the dispatch of electronic communication occurs when it is capable of being retrieved by the addressee.

Time of receipt of electronic communications

22.(1) If the addressee has designated an information system for the purpose of receiving electronic communications, the time of receipt of an electronic communication shall be determined as follows -

(a) at the time when the electronic communication enters the designated information system of the addressee; or

(b) when the electronic communication is sent to an information system of the addressee that is not the designated information system, at the time when –

(i) the addressee becomes aware that the electronic communication has been sent to that information system, and

(ii) the electronic communication is capable of being retrieved by the addressee.

(2) An electronic communication is deemed to be capable of being retrieved by the addressee when it reaches the addressee's electronic address.

(3) If the addressee has not designated an information system, receipt occurs when the electronic communication is retrieved by the addressee, or should reasonably have been retrieved by the addressee.

Place of dispatch and receipt of electronic communications

23.(1) An electronic communication is deemed to have been dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business.

(2) For the purposes of this section -

(a) if the originator or the addressee has more than one place of business, the place of business is -

(i) that place which has the closest relationship to the underlying transaction having regard to the circumstances known to or contemplated by the parties at any time before or at the conclusion of the contract, or

(ii) where there is no underlying transaction, the principal place of business; and

(b) if the originator or the addressee does not have a place of business, reference is to be made to that

person’s habitual residence.

(3) This section shall apply notwithstanding that the place where the information system which supports an electronic address is located is different from the place where the electronic communication is deemed to be received.

Acknowledgment of receipt

24.(1) This section shall apply where, on or before sending an electronic communication, or by means of that electronic communication, the originator has requested or has agreed with the addressee that receipt of the communication be acknowledged and is not intended to deal with the legal consequences that may flow either from that electronic communication or from the acknowledgement of its receipt.

(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 sufficient to indicate to the originator that the electronic communication has been received.

(3) Where the originator has stated that the electronic communication is conditional on receipt of the acknowledgement, the electronic communication shall be treated as if it has never been sent until the acknowledgement is received.

(4) Where the originator has not stated that the electronic communication 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 the originator may, within a reasonable time -

(a) 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)*, upon notice to the addressee, treat the electronic communication as if it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it shall be presumed that the related electronic message was received by the addressee except that the presumption shall not imply that the electronic communication corresponds to the message received.

(6) Where the received acknowledgement states that the related electronic communication has met technical requirements either agreed upon or set out in applicable standards, it shall be presumed that those requirements have been met.

Part V – *Secure Electronic Signatures*

Requirements for electronic signatures

25.(1) An electronic signature shall be considered to be reliable for the purpose of satisfying the requirements of this Act where –

(a) the signature creation data is, within the context in which it is used, linked to the signatory and to no other person;

(b) the signature creation data 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) the purpose of a 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.

(2) Subsection (1) shall not limit the ability of any person –

(a) to establish in any other way, for the purpose of satisfying the requirement referred to in section 6, the reliability of an electronic signature; or

(b) to adduce evidence of the non-reliability of an electronic signature.

Secure electronic signatures

26.(1) The Minister may prescribe methods of accrediting products or services required to authenticate and recognize secure electronic signatures which satisfy the provisions of this Act.

(2) The Communications Regulatory Authority shall be responsible for the accreditation of certification service providers and recognition of foreign certificates.

(3) Any method prescribed under subsection (1) shall be consistent with recognised international standards.

(4) Where a secure electronic signature is or has been used, such signature shall be regarded as a valid electronic signature and to have been applied properly, unless the contrary is proved.

Conduct of signatory

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

(a) exercise reasonable care to avoid unauthorized access and use of its signature creation data;

(b) without undue delay, utilize means made available by the certification service provider in terms of section 28 or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature if –

(i) the signatory knows that the signature creation data has been compromised, or

(ii) circumstances exist which are known to the signatory to give rise to a substantial risk that the signature creation data 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 signatory that are relevant to the certificate throughout its life cycle or that are to be included in the certificate.

(2) A signatory shall bear the legal consequences of its failure to comply with the requirements of subsection (1).

Conduct of certification service provider

28.(1) Where a certification service provider provides services to support an electronic signature under this Act, that certification service provider shall –

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

(b) exercise reasonable care to ensure the accuracy and completeness of all material representations made by it that are relevant to the certificate throughout its life cycle or that are included in the certificate;

(c) provide reasonably accessible means that enable a relying party to ascertain from the certificate -

(i) the identity of the certification service provider,

(ii) that the signatory that is identified in the certificate had control of the signature creation data at the time when the certificate was issued, and

(iii) that signature creation data was valid at or before the time when the certificate was issued;

(d) provide reasonably accessible means that enable a relying party to ascertain, where relevant, from the certificate or otherwise –

(i) the method used to identify the signatory,

(ii) any limitation on the purpose or value for which the signature creation data or the certificate may be used,

(iii) that the signature creation data is valid and has not been compromised,

(iv) any limitation on the scope or extent of liability stipulated by the certification service provider,

(v) whether means exist for the signatory to give notice in terms of section 27(1)*(b)*, or

(vi) whether a timely revocation service is offered;

(e) where services under paragraph *(d)* (v) are offered, provide a means for the signatory to give notice in terms of section 27(1)*(b)* and, where services under subparagraph *(d)* (vi) are offered, ensure the availability of a timely revocation service; and

(f) utilize reliable and secure systems, procedures and human resources in performing its services.

(2) A certification service provider shall bear the legal consequences of its failure to satisfy the requirements of subsection (1).

Reliable and secure systems

29. For purposes of section 28(1)*(f),* in determining whether, or to what extent, any systems, procedures and human resources utilized by a certification service provider are reliable and secure, regard may be had to the following factors -

(a) financial and human resources, including existence of assets;

(b) quality of hardware and software systems;

(c) procedures for processing of certificates and applications for certificates and retention of records;

(d) availability of information to signatories identified in certificates and to potential relying parties;

(e) regularity and extent of audit by an independent body;

(f) the existence of a declaration by the Communications Regulatory Authority or the certification service provider regarding compliance with or existence of any of the factors set out in paragraphs (a) to (e); or

(g) any other relevant factor.

Conduct of relying

30. A relying party shall bear the legal consequences of its

party

failure -

(a) to take reasonable steps to verify the reliability of an electronic signature; or

(b) where an electronic signature is supported by a certificate, to take reasonable steps –

(i) to verify the validity, suspension or revocation of the certificate, and

(ii) to observe any limitation with respect to the certificate.

Recognition of foreign certificates and electronic signatures

31.(1) In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had –

(a) to the geographic location where the certificate is issued or the electronic signature was created or used; or

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

(2) A certificate issued outside Botswana shall have the same legal effect in Botswana as a certificate issued in Botswana if it offers a substantially equivalent level of reliability.

(3) An electronic signature created or used outside Botswana shall have the same legal effect in Botswana as an electronic signature created or used in Botswana if it offers a substantially equivalent level of reliability.

(4) In determining whether a certificate or an electronic signature offers a substantially equivalent level of reliability for the purposes of subsections (2) or (3), regard shall be had to recognized international standards and to any other relevant factors.

(5) Where, notwithstanding subsections (2), (3) and (4), parties agree as between themselves, to the use of certain types of electronic signatures or certificates, that agreement shall be recognized as sufficient for the purposes of cross-border recognition, unless that agreement would not be valid or effective under applicable law.

Application of Part

32.(1) Subject to subsection (2), this Part shall only apply to electronic transactions.

(2) This Part shall not apply to electronic transactions –

(a) by way of an auction;

(b) for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;

(c) for services which began with the consumer's consent before the end of the seven-day period referred to in section 35(1);

(d) where the price for the supply of goods or services is dependent on fluctuations in the financial markets and which cannot be controlled by the supplier;

(e) where the goods –

(i) are made to the consumer's specifications,

(ii) are clearly personalised,

(iii) by reason of their nature cannot be returned, or

(iv) are perishable and are likely to deteriorate or expire rapidly;

(f) where audio or video recordings or computer software was unsealed by the consumer;

(g) for the sale of newspapers, periodicals, magazines or books;

(h) for the provision of gaming or lottery services;

(i) for on-line gambling; and

(j) for the provision of accommodation, transport, catering or leisure services and where the supplier undertakes, when the transaction is

concluded, to provide these services on a specific date or within a specific period.

Supplier to provide information

33. (1) A supplier offering goods or services for sale, for hire or for exchange by way of an electronic transaction shall make the following information available to consumers –

(a) its full contact details, including its place of business, email address, mobile number, and telefax numbers;

(b) a sufficient description of the main characteristics of the goods or services offered by that supplier to enable a consumer to make an informed decision on the proposed electronic transaction;

(c) the full price of the goods or services, including transport costs, taxes and any other fees or costs;

(d) information regarding the payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned;

(e) any terms of agreement including any guarantees that will apply to the transaction and how those terms will be accessed, stored and reproduced electronically by the consumer; and

(f) the manner and period within which consumers can access and maintain a full record of the transaction.

(2) The supplier shall provide a consumer with an opportunity –

(a) to review the entire electronic transaction;

(b) to correct any mistakes; and

(c) to withdraw from the transaction, before finally placing any order.

(3) If a supplier fails to comply with the provisions of subsection (1) or (2), the consumer may cancel the transaction within 14 days of receiving the goods or services under the transaction.

(4) If a transaction is cancelled in terms of subsection (3) –

(a) the consumer shall return the goods or the performance of the supplier or, where applicable, cease using the services performed; and

(b) the supplier shall refund all payments made by the consumer minus the direct cost of returning the goods.

Performance

34.(1) The supplier shall execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise.

(2) Where a supplier has failed to execute the order within 30 days or within the agreed period, the consumer may cancel the agreement by giving seven days' written notice to the supplier.

(3) If a supplier is unable to perform in terms of the agreement on the grounds that the goods or services ordered are unavailable, the supplier shall immediately notify the consumer of this fact and refund any payments within 30 days after the date of such notification.

Cooling-off

35. (1) A consumer is entitled to cancel without reason and without penalty any transaction and any related credit agreement for the supply –

(a) of goods within seven days after the date of the receipt of the goods; or

(b) of services within seven days after the date of the conclusion of the agreement.

(2) Where a consumer cancels a transaction in terms of subsection (1) the only charge that may be levied on the consumer is the direct cost of returning the goods.

(3) If payment for the goods or services has been effected prior to a consumer exercising a right referred to in subsection (1), the consumer is entitled to a full refund of such payment, which refund shall be made within 30 days of the date of cancellation.

(4) This section shall not be construed as prejudicing the

rights of a consumer provided for in any other law.

Applicability of foreign law

36. The protection provided to consumers in this Part, applies irrespective of the legal system applicable to the agreement in question.

Non-exclusion

37. The provisions of this Part shall not be deviated from by agreement.

Part VII - *On-Line Marketing*

Unsolicited commercial communications

38. (1) An originator who carries out marketing by means of electronic communication shall provide the addressee with –

(a) the originator's identity and contact details including its place of business, e-mail, addresses and telefax number;

(b) a valid and operational opt-out facility from receiving similar communications in future; and

(c) the identifying particulars of the source from which the originator obtained the addressee's personal information.

(2) Unsolicited commercial communications may only be sent to addressees where the opt-in requirement is met.

(3) The opt-in requirement is deemed to have been met where -

(a) the addressee's e-mail address and other personal information was collected by the originator of the message "in the course of a sale or negotiations for a sale";

(b) the originator only sends promotional messages relating to its "similar products and services" to the addressee;

(c) when the personal information and address was collected by the originator, the originator offered the addressee the opportunity to opt-out, free of charge except for the cost of transmission, and the addressee declined to opt-out; and

(d) the opportunity to opt-out is provided by the

originator to the addressee with every subsequent message.

(4) No contract is formed where an addressee does not respond to an unsolicited commercial communication.

(5) An originator who fails to provide the addressee with an operational opt-out facility in terms of this section commits an offence and is liable to a fine not exceeding P10 000, or to imprisonment for a term not exceeding five years, or to both.

(6) Any originator who persists in sending unsolicited commercial communications to an addressee who has opted-out from receiving any further electronic communications from the originator through the originator's opt-out facility commits an offence and is liable to a fine not exceeding P50 000, or to imprisonment for a term not exceeding eight years, or to both.

PART VIII - *Service Providers*

Application

39. (1) Nothing in this Part shall affect –

(a) any obligation arising from a contract or agreement;

(b) the obligation of a service provider under the Communications Regulatory Authority Act;

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

Cap. 68:02

(d) any liability of a service provider under the Copyright and Neighbouring Rights Act 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.

(2) In this Part –

"performance" shall have the same meaning provided for in section 2 of the Copyright and Neighbouring Rights Act; and "third party" in relation to a service provider means a person over whom the provider has no control.

Mere conduit

40. (1) A service provider shall not be subject to any civil or criminal liability in respect of third-party material in the form of electronic communications to which he or she merely provides access to or for operating facilities for information system services for the transmitting, routing or storage of electronic communications via an information system under its control, where the service provider -

(a) does not initiate the transmission;

(b) does not select the addressee;

(c) performs the functions in an automatic, technical manner without selection of the data; and

(d) does not modify the data contained in the transmission.

(2) The acts of transmission, routing and of provision of access referred to in subsection (1) include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place –

(a) for the sole purpose of carrying out the transmission in the information system;

(b) in a manner that makes it ordinarily inaccessible to anyone other than anticipated addressees; and

(c) for a period no longer than is reasonably necessary for the transmission.

Caching

41. (1) A service provider shall not be subject to any civil liability in respect of third-party material in the form of electronic communications for the automatic, intermediate and temporary storage of that data, where the purpose of storing such data is to make the onward transmission of the data more efficient to other addressees of the service upon their request, where the service provider –

(a) does not modify the data;

(b) complies with conditions on access to the data;

(c) complies with rules regarding the updating of the data, specified in a manner widely recognized and used in the industry;

(d) does not interfere with the lawful use of right management information, widely recognized and used in the industry, to obtain information on the use of the data; and

(e) removes or disables access to the data it has stored upon receiving a take-down notice referred to in section 44.

(2) Notwithstanding subsection (1), a court may order a service provider to terminate or prevent unlawful activity in terms of any other law.

Hosting

42. (1) A service provider is not liable for civil liability in respect of third-party material in the form of electronic communications where the service provider provides a service at the request of the addressee of the service that consists of the storage of data provided by the addressee of the service, where the service provider –

(a) does not have actual knowledge that the electronic communication or an activity relating to the electronic communication is infringing the rights of a third party;

(b) is not aware of facts or circumstances from which the infringing activity or the infringing nature of the electronic communication is apparent; and

(c) upon receipt of a take-down notification from the aggrieved party referred to in section 44, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section shall not apply to a service provider unless it has designated an agent to receive notifications of infringement and has provided through its service, including on its websites in locations accessible to the public, the contact details of the agent.

(3) Subsection (1) shall not apply when the addressee of the service is acting under the authority or the control of the service provider.

Information location tools

43. (1) A service provider is not liable for civil liability in respect of third-party material in the form of electronic communications if the service provider refers or links users to a web page containing an infringing electronic communication or an infringing activity, by using information location tools, including a directory, index, reference, pointer, or hyperlink, where the service provider –

(a) does not have actual knowledge that the electronic communication or an activity relating to the electronic communication is infringing the rights of that person;

(b) is not aware of the facts or circumstances which evidences the infringing activity or the infringing nature of the electronic communication;

(c) does not receive a financial benefit directly attributable to the infringing activity; and

(d) removes, or disables access to the reference or link to the electronic communication or activity within a reasonable time after being informed that the electronic communication or the activity relating to such electronic communication infringes the rights of a person.

Take-down notification

44.(1) For the purposes of this Part, take down notifications shall be administered by the Communications Regulatory Authority and a notification of any unlawful activity shall be in the form of an electronic communication and it shall be addressed to the Communications Regulatory Authority and the service provider or its designated agent.

(2) The notification shall include -

(a) the full names and address of the complainant;

(b) the signature of the complainant;

(c) identification of the right that has allegedly been infringed;

(d) identification of the material or activity that is claimed to be the subject of unlawful activity;

(e) the remedial action required to be taken by the

service provider in respect of the complaint;

(f) telephonic and electronic contact details, if any, of the complainant;

(g) a statement that the complainant is acting in good faith; and

(h) a statement by the complainant that the information in the take-down notification is to his or her knowledge true or correct.

(3) Any person who lodges a notification of unlawful activity with the Communications Regulatory Authority and a service provider or its designated agent knowing that it materially misrepresents the facts shall be liable for damages for wrongful take-down.

(4) A service provider shall not be liable for wrongful take-down in response to a notification of unlawful activity which complies with subsection (1).

Monitoring

45.(1) A service provider shall not, in compliance with the provisions of this part, be generally obliged to –

(a) monitor the data which it transmits or stores; or

(b) actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may, subject to the provisions of any other law, prescribe procedures for service providers to –

(a) inform the competent public authorities of alleged illegal activities undertaken or information provided by addressees of their service; and

(b) communicate to the competent authorities, at their request, information enabling the identification of addressees of their service.

PART IX – *General Provisions*

Offences and penalties

46. Any person who contravenes or fails to comply with any provision of this Act for which a penalty has not been provided for elsewhere in this Act commits an offence and is

liable to a fine not exceeding P10 000, or to imprisonment for a term not exceeding five years, or to both.

Regulations

47.(1) The Minister may make regulations for the better carrying out of the provisions of this Act and may impose penalties for breach by any person of any such regulations.

(2) Without prejudice to the generality of subsection (1), the Minister may make regulations relating to -

(a) the accreditation of methods used for secure electronic signatures;

(b) methods used for recognition of secure electronic signatures;

(c) the licensing or registration of certification service providers;

(d) requirements for secure signature creation devices;

(e) requirements for certificates; and

(f) any other matter which requires to be prescribed under this Act.