Establishment of Harmonized Policies for the ICT Market in the ACP Countries

Electronic Transactions and Electronic Commerce:

Southern African Development Community (SADC) Model Law

HIPSSA

Harmonization of ICT Policies in Sub-Saharan Africa

Disclaimer

This document has been produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

The designations employed and the presentation of material, including maps, do not imply the expression of any opinion whatsoever on the part of ITU concerning the legal status of any country, territory, city or area, or concerning the delimitations of its frontiers or boundaries. The mention of specific companies or of certain products does not imply that they are endorsed or recommended by ITU in preference to others of a similar nature that are not mentioned.

Please consider the environment before printing this report.

Foreword

Information and communication technologies (ICTs) are shaping the process of globalisation. Recognising their potential to accelerate Africa's economic integration and thereby its greater prosperity and social transformation, Ministers responsible for Communication and Information Technologies meeting under the auspices of the African Union (AU) adopted in May 2008 a reference framework for the harmonization of telecommunications/ICT policies and regulations, an initiative that had become especially necessary with the increasingly widespread adoption of policies to liberalise this sector.

Coordination across the region is essential if the policies, legislation, and practices resulting from each country's liberalization are not to be so various as to constitute an impediment to the development of competitive regional markets.

Our project to 'Support for Harmonization of the ICT Policies in Sub-Sahara Africa' (HIPSSA) has sought to address this potential impediment by bringing together and accompanying all Sub-Saharan countries in the Group of African, Caribbean and Pacific States (ACP) as they formulate and adopt harmonized ICT policies, legislation, and regulatory frameworks. Executed by the International Telecommunication Union (ITU), co-chaired by the AU, the project has been undertaken in close cooperation with the Regional Economic Communities (RECs) and regional associations of regulators which are members of the HIPSSA Steering Committee. A global steering committee composed of the representatives of the ACP Secretariat and the Development and Cooperation – EurepeAid (DEVCO, European Commission) oversees the overall implementation of the project.

This project is taking place within the framework of the ACP Information and Telecommunication Technologies (@CP-ICT) programme and is funded under the 9th European Development Fund (EDF), which is the main instrument for providing European aid for development cooperation in the ACP States, and co-financed by the ITU. The @CP-ICT aims to support ACP governments and institutions in the harmonization of their ICT policies in the sector by providing high-quality, globally-benchmarked but locally-relevant policy advice, training and related capacity building.

All projects that bring together multiple stakeholders face the dual challenge of creating a sense of shared ownership and ensuring optimum outcomes for all parties. HIPSSA has given special consideration to this issue from the very beginning of the project in December 2008. Having agreed upon shared priorities, stakeholder working groups were set up to address them. The specific needs of the regions were then identified and likewise potentially successful regional practices, which were then benchmarked against practices and standards established elsewhere.

These detailed assessments, which reflect sub-regional and country-specific particularities, served as the basis for the model policies and legislative texts that offer the prospect of a legislative landscape for which the whole region can be proud. The project is certain to become an example to follow for the stakeholders who seek to harness the catalytic force of ICTs to accelerate economic integration and social and economic development.

I take this opportunity to thank the European Commission and ACP Secretariat for their financial contribution. I also thank the Economic Community of West African States (ECOWAS), West African Economic and Monetary Union (UEMOA), Economic Community of Central African States (ECCAS), Economic and Monetary Community of Central Africa (CEMAC), East African Community (EAC), Common Market for Eastern and Southern Africa (COMESA), Common Market for Eastern and Southern Africa (COMESA), Southern African Development Community (SADC), Intergovernmental Authority on Development (IGAD), Communication Regulators' Association of Southern Africa (CRASA), Telecommunication Regulators' Association of Central Africa (ARTAC), United Nations Economic Commission for Africa (UNECA), and West Africa Telecommunications Regulators' Association (WATRA), for their contribution to this work. Without political will on the part of beneficiary countries, not much would have been achieved. For that, I express my profound thanks to all the ACP governments for their political will which has made this project a resounding success.

Brahima Sanou
BDT, Director

Acknowledgements

The present document represents an achievement of a regional activity carried out under the HIPSSA project ("Support to the Harmonisation of ICT Policies in Sub-Sahara Africa") officially launched in Addis Ababa in December 2008.

In response to both the challenges and the opportunities of information and communication technologies' (ICTs) contribution to political, social, economic and environmental development, the International Telecommunication Union (ITU) and the European Commission (EC) joined forces and signed an agreement (ITU-EC Project) aimed at providing "Support for the Establishment of Harmonized Policies for the ICT market in the ACP", as a component of the Programme "ACP-Information and Communication Technologies (@CP-ICT)" within the framework of the 9th European Development Fund (EDF), i.e., ITU-EC-ACP project.

This global ITU-EC-ACP project is being implemented through three separate sub-projects customized to the specific needs of each region: Sub-Saharan Africa (HIPSSA), the Caribbean (HIPCAR), and the Pacific Island Countries (ICB4PAC).

As members of the HIPSSA Steering Committee co-chaired by the African Union's Commission (AUC) and the ITU, the Southern African Development Community (SADC) Secretariat and Communication Regulators' Association of Southern Africa (CRASA) Secretariat provided guidance and support to the consultants, Prof. Tana Pistorious and Mr. Adam Mambi who prepared the draft document. This draft document has been reviewed, discussed and validated by broad consensus by participants of the workshop organised in collaboration with CRASA and SADC Secretariats held in Gaborone, Botswana from 27 February to 3 March 2012. It was further adopted by the SADC Ministers responsible for Telecommunications, Postal and ICT at their meeting in Mauritius in November 2012.

ITU would like to thank the workshop delegates from the SADC ICT and telecommunications ministries, CRASA regulators, academia, civil society, operators and regional organisations for their hard work and commitment in producing the contents of the final report. The contributions from the SADC and CRASA Secretariats are gratefully acknowledged.

Without the active involvement of all of these stakeholders, it would have been impossible to produce a document such as this, reflecting the overall requirements and conditions of the SADC region while also representing international best practice.

The activities have been implemented by Ms. Ida Jallow, responsible for the coordination of the activities in Sub-Saharan Africa (HIPSSA Senior Project Coordinator), and Mr. Sandro Bazzanella, responsible for the management of the whole project covering Sub-Saharan Africa, Caribbean and the Pacific (ITU-EC-ACP Project Manager) with the overall support of Ms. Hiwot Mulugeta, HIPSSA Project Assistant, and of Ms. Silvia Villar, ITU-EC-ACP Project Assistant. The work was carried out under the overall direction of Mr. Cosmas Zavazava, Chief, Project Support and Knowledge Management Department. The document was developed under the direct supervision of the then HIPSSA Senior Project Coordinator, Mr. Jean-François Le Bihan, and has further benefited from the comments of the ITU Telecommunication Development Bureau's (BDT) Regulatory and Market Environment (RME), Special Initiatives and Strategies (SIS), and from ICT Applications and Cybersecurity (CYB) Divisions at the ITU. The team at ITU's Publication Composition Service was responsible for its publication.

Table of contents

Table of contents

Table of contents

PREAMBLE

The digitization of information and the rapid growth of network connectivity have affected our social, political, and economic spheres and changed the way we communicate and do business. The continuing development of the Internet and its associated applications has created a variety of new opportunities for Africa. The Internet has become a vehicle for tremendous economic growth through the development of electronic commerce (e-commerce). The fundamental benefit of e-commerce is enhanced communication, which allows for simplicity, flexibility and new business opportunities. These developments have dramatically and irrevocably altered the needs of stakeholders: governments, businesses and consumers alike.

The principles of contract law are old: they were formed in a paper-based world that ran on paper and ink. The meeting of minds in cyberspace was never envisaged, and the validity and effect of using electronic messages in commercial communications were never contemplated. Requirements such as writing and signature cannot be translated to the virtual and paperless world of e-commerce without legislative intervention. Other common problems of e-contracting include: the legal value and validity of electronic communications; complying with formalities; determining the time and place of the conclusion of a contract; and the validity of automated transactions.

A legal problem that flows from the use of e-communications is the admissibility and evidentiary weight of electronic evidence. Conventional time and place have been replaced by 'any moment, any place', in an interconnected world. Both the trader and consumer have taken on new roles. The electronic consumer cannot sample, for example, the fresh produce or test the strength of a container before they click to purchase a product. Consumers, generally, do not trust the confidentiality, security and electronic-payment mechanisms. The creators of website shopping malls are faced with the challenge of designing their sites in order to effectively contract with customers. These problems collectively contribute to a lack of confidence on the part of both consumers and businesses to conduct business online.

In the digital environment, the technical role played by online service providers (OSPs), also referred to as Internet service providers (ISPs), establishes their potential liability. Liability may be imposed on them by the law regarding privacy, trade secrets, content restrictions, security, intellectual-property protection, product liability, defamation, and the like. These problems contribute to a further lack of confidence on the part of consumers and business in Internet commerce.

In order to flourish, e-commerce requires an accessible, predictable, safe and transparent trading environment, which operates across territorial borders and jurisdictions. The advent of the use of electronic communications for commercial transactions posed unexpected and complex legal problems for SADC countries, as it did for countries worldwide. The SADC Model Law on Electronic Transactions and E-commerce provides a tool that Member States can use to create a more secure legal environment for electronic transactions and e-commerce. It seeks to enhance regional integration and has adopted the best practices and collective efforts of Member States to address the legal aspects of e-transactions and e-commerce. The Model Law is expressed in a technologically neutral manner so that it can be applied to existing technologies as well as future ones yet to be developed.

This Model Law addresses the scope of application of key concepts and proposes neutral definitions for them. The legal recognition of electronic communications and the legal effect of electronic communications are addressed. Clear rules for electronic transactions are adopted. E-commerce issues such as the attribution of electronic communications and electronic signatures, and the admissibility and evidentiary weight of electronic evidence are addressed. The obligations of online suppliers are addressed. These include the type of information made available to consumers on the information system where such goods or services are offered, and a consumer's right to a cooling-off period, review of a transaction, withdrawal from a transaction, and the performance, correction or cancellation of a transaction for goods and services. Lastly, service providers' liability is addressed.

Part I

PART I: GENERAL ENABLING PROVISIONS

CHAPTER 1: DEFINITIONS AND INTERPRETATION

Section 1: Definitions

For the purposes of this Model Law:

(1) **"addressee"** of 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;

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

(3) "**cache**" means high-speed memory that stores data for relatively short periods of time in an information system in order to speed up data transmission or processing;

(4) **"consumer**" means a natural person and/or a non-profit organisation that purchases goods and services for the direct satisfaction of individual needs or wants or the collective needs of members of a community;

or

"**consumer**" means any natural person who enters or intends entering into an electronic transaction with a supplier as the end user of the goods or services offered by that supplier;

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

(6) **"direct costs"** mean costs incurred such as transport costs or postage when returning goods or services but excludes any handling fees;

(7) "**e-government services**" means any public service provided by means of electronic communications by any public office or any automated means intended for public service;

(8) **"electronic record"** means a record in the form of a stored electronic communication;

(9) **"electronic communication"** means communication made by means of a data message;

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

(11) **"electronic signature"** means data, including an electronic sound, symbol or process, executed or adopted to identify a party and to indicate that party's approval or intention in respect of the information contained in the electronic communication and which is attached to or logically associated with such electronic communication;

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

(13) **"intermediary"** with respect 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;

(14) **"information system"** means a device or group of interconnected or related devices, including the Internet, one or more which, pursuant to a program, performs automatic processing of data/or any other functions;

(15) **"information system services"** means providing the connection and network facilities necessary for transmitting, hosting and routing 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;

(16) **"originator"** of 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 it does not include a person or party acting as an intermediary with respect to that electronic communication;

(17) "**place of business**" means any place where a 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;

(18) **"program"** means a set of instructions fixed or stored in any manner or form and which, when used directly or indirectly in an automated system, directs its operations to bring about a result;

(19) **"secure electronic signature"** means a signature duly recognised in terms of subsection 8(1), which is created and can be verified through the application of a security procedure or combination of security procedures that ensures that an electronic signature:

a. is unique to the signer for the purpose for which it is used;
b. can be used to identify objectively the signer of the electronic communication;
c. was created and affixed to the electronic communication by the signer or using a means under the sole control of the signer; and
d. was created and is linked to the electronic communication to which it relates in a manner such that any changes to the electronic communication would be revealed.

(20) **"service provider"** means a person or party that makes information system services available.

Section 2: Interpretation

(1) Where any law grants a public body the authority to prescribe by regulation, such authority of the public body shall be deemed to have been extended to prescribe by means of electronic communications for any matter provided for in such law.

(2) Any reference in this Model Law to law shall include reference to all sources of law, including statutes, regulations or other subordinate legislation issued in terms thereof as well as common law and customary law, unless specifically provided otherwise.

Section 3: Scope of application

(1) This Model Law shall apply in respect of any electronic transaction or electronic communication used or intended to be used in relation to an electronic transaction, except where, and if applicable, to the extent, that it is excluded in subsection 6(4) and subsection 7(5) of this Model Law.

(2) Nothing in this Model Law shall be construed as:

a. requiring any person to use or to accept electronic communications; or

b. prohibiting a person engaging in an electronic transaction or electronic commerce from establishing reasonable requirements about the manner in which it will accept electronic communications.

(3) Notwithstanding the provisions of subsection (2) above, a person's agreement to use or accept electronic communications may be inferred from such person's conduct.

(4) Parties may agree to exclude the application of this Model Law between themselves (*inter partes*) or they may derogate from and or vary the effect of sections 6 and 7 and/or Chapter 5 by agreement.

CHAPTER 2: LEGAL RECOGNITION OF ELECTRONIC COMMUNICATIONS

Section 4: Legal recognition of electronic communications

A data message shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic communication.

Section 5: Recognition by parties of electronic communications

Between the originator and the addressee of an electronic communication, a declaration of will, other statement or action shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of an electronic communication.

CHAPTER 3: LEGAL EFFECT OF ELECTRONIC COMMUNICATIONS

Section 6: Writing

(1) Where a law requires information to be in writing, that requirement is met by an electronic communication if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Subsection 1 applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) For the purposes of this section, an electronic communication shall include:

a. making an application;

b. making or lodging a claim;

c. giving, sending or serving a notification, statement or declaration;

d. lodging a return;

e. making a request;

f. making a declaration or demand;

g. lodging or issuing a certificate;

h. making, varying or cancelling an election;

i. lodging an objection; giving a statement of reasons; and

j. such other action/s as may be prescribed.

(4) The provisions of this section shall not apply to the requirement of writing for:

a. a contract for the alienation of immovable property;
b. a contract for the long-term lease of immovable property in excess of 20 years;
c. the execution, retention and presentation of a will or codicil;
d. the execution of a bill of exchange; and
e. such other documents or instrument as may be prescribed by a Member State.

Section 7: Signature

(1) If a law requires the signature of a person, an electronic signature will be deemed to be valid, provided the electronic signature complies with the requirements as prescribed by Regulation.

(2) The requirements for an electronic signature referred to in subsection 1 above will be met if:

a. the method is used to identify the person and to indicate the person's intention in regard to the information communicated; and
b. at the time the method was used, the method was as reliable as was appropriate for the purposes for which the information was communicated in light of all the relevant circumstances.

(3) Where two persons or parties agree to make use of electronic signatures they may agree to use any method of signing as they deem appropriate.

(4) Subsection (1) applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(5) The provisions of this section do not apply to the requirement for a signature for the following acts:

a. the offer or acceptance of a contract for the alienation of immovable property;
b. the signing of a contract for the long-term lease of immovable property in excess of 20 years;
c. the execution, retention and presentation of a will or codicil;
d. the execution of a bill of exchange; and
e. such other laws or statutes as may be prescribed by a Member State.

Section 8: Creation and recognition of secure electronic signature

(1) Member States may by Regulation provide that accredited authentication products or services are recognised as a secure electronic signature and may prescribe certain standards and licensing procedures for such products or services including the recognition of foreign, secure electronic signatures.

(2) Any recognition granted in terms of this sub-section 1 should be consistent with generally recognized international technical standards.

(3) Where a secure electronic signature has been used, the signature is regarded as being a valid electronic signature and having been applied properly, unless the contrary is proved.

(4) Electronic signatures that are not secure electronic signatures are not subject to the presumptions set out in subsection 3 above and section 18 below.

Section 9: Incorporation by reference

Information shall not be denied legal effect, validity or enforceability solely on the ground that it is not contained in the electronic communication purporting to give rise to such legal effect, validity or enforceability, but is merely referred to in that electronic communication.

Part II

PART II: ELECTRONIC TRANSACTIONS

CHAPTER 4: LEGAL RECOGNITION OF ELECTRONIC TRANSACTIONS

Section 10: Formation and validity of contracts

(1) Where electronic communications are used in the formation of a contract, that contract shall not be denied legal effect, validity or enforceability on the sole ground that an electronic communication was used to make an offer or to accept an offer for that purpose.

(2) 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) 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.

Section 11: Variation by agreement

The provisions under Chapter 5 shall apply, unless the parties involved in generating, sending, receiving, storing or otherwise processing electronic communications, have agreed otherwise.

CHAPTER 5 : TIME AND PLACE OF DISPATCH AND RECEIPT OF ELECTRONIC COMMUNICATIONS

Section 12 : Time of dispatch of electronic communications

(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 an electronic communication occurs when it is capable of being retrieved by the addressee.

Section 13 : Time of receipt of electronic communications

(1) If the addressee has designated an information system for the purpose of receiving electronic communications, the time of receipt of an electronic communication is determined as follows:

a. at the time when the electronic communication enters the designated information system; 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 the electronic communication is 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.

(2) An electronic communication is deemed to be capable of being retrieved by the addressee for the purposes of subsection 12(2) and paragraph b of subsection 13(1) 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.

Section 14: Place of dispatch and receipt of electronic communications

(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 subsection (1) above:

a. if the originator or the addressee has more than one place of business, the place of business is:
    i. that which has the closest relationship to the underlying transaction having regard to the circumstances known 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.
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 supporting an electronic address is located may be different from the place where the electronic communication is deemed to be dispatched or deemed to be received under this section.

Section 15: Time of contract formation

(1) Where parties conclude a contract by means of electronic communications, such contract is 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 that it is received by the offeror.

Section 16: Automated message systems

(1) 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.

(2) 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 electronic communication in which the input error was made if:

a. the person, or the party on whose behalf that person was acting, notifies the other party of the error as soon as possible after having learned 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. the person, or the party on whose behalf that person was acting, 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;

c. the person, or the party on whose behalf that person was acting, 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;

d. 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 such payment, and the refund shall be made within 30 days of the date of cancellation.

(3) Nothing in this section affects the application of any rule of law that may govern the consequences of any errors made during the formation or performance of the type of contract in question other than an input error that occurs in the circumstances referred to in subsection 2.

Part III

PART III: ELECTRONIC COMMERCE

CHAPTER 6: ATTRIBUTION

Section 17: Attribution of electronic communications

An electronic communication is that of the originator if it was sent by:

(a) the originator personally;

(b) a person who had authority [is duly authorised] 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 is proved that the information system did not properly execute such programming.

Section 18: Attribution of secure electronic signatures

A secure electronic signature is deemed to have been applied by the holder of the secure electronic signature, unless the contrary is proved.

CHAPTER 7: ADMISSABILITY AND EVIDENTIARY WEIGHT OF ELECTRONIC COMMUNICATIONS

Section 19: Original information

(1) Where the law requires information to be presented in its original form, that requirement is met 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; and

(b) where it is required that information be presented, that information is capable of being displayed in the form of an electronic communication to the person to whom it is to be presented.

(2) Sub-section 1 applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

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

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

Section 20: Admissibility and evidential weight of electronic communications

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of an electronic communication in evidence:

a. on the sole ground that it is in the form of 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 electronic communication 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 its originator was identified; and

d. any other relevant factor.

(4) An electronic communication made by or on behalf of a person in the ordinary course of business, or a copy or printout of, or an extract from such electronic communication certified to be correct, is admissible in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, as evidence of the facts contained in such record, copy, printout or extract against any person, provided:

a. the affidavit is made by the person who was in control of the system at the time when the electronic communication was created;

b. the affidavit contains sufficient information on the following:

i. the reliability of the manner in which the electronic communication was generated, stored or communicated;

ii. the reliability of the manner in which the integrity of the electronic communication was maintained;

iii. the manner in which the originator of the electronic communication was identified; and

iv. the reliability of the information system.

Section 21: Retention of records

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by electronic record retention, providing that the following conditions are satisfied:

a. the electronic record contained therein is an electronic communication;

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

c. such electronic record is retained in a form that enables the identification of the origin and destination of an electronic record or electronic communication and the date and time when it was first generated, sent or received, and the date and time it was first retained.

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

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

Section 22: Production of document or information

(1) Where a law requires a person 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 assuring 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 therein would be readily accessible so as to be usable for subsequent reference.

(2) For the purposes of subsection 1, the integrity of the information contained in a document is maintained if the information has remained complete and unaltered, except for

a. the addition of any endorsement; or

b. any immaterial change, which arises in the normal course of communication, storage or display.

Section 23: Notarisation, acknowledgement and certification

(1) Where a law requires a signature, statement or document to be notarised, acknowledged, verified or made under oath, that requirement is met if the secure electronic signature of the person authorised to perform those acts 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 printout 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 thereof and the certification is confirmed by the use of a secure electronic signature.

Section 24: Other requirements

(1) A requirement in a law for multiple copies of a document to be submitted to a single addressee at the same time is satisfied by the submission of a single electronic communication that is capable of being reproduced by that addressee.

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

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

(4) Where any law requires or permits a person to send a document or information by post or similar service, that requirement is met if an electronic form of that document or information is sent to the electronic address provided by the addressee.

Part IV

PART IV: CONSUMER PROTECTION

CHAPTER 8: THE PROTECTION OF ONLINE CONSUMERS

Section 25: Obligations of the supplier

(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, e-mail addresses and telefax number(s);

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

(2) The supplier shall provide the 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 sub-sections 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 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.

Section 26: Performance

(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 with seven days' written notice.

(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.

Part IV

Section 27: Cooling-off

(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) 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 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.

(5) This section shall not apply to electronic transactions:

a. for financial services, including but not limited to investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;

b. by way of an auction;

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

d. for services which began with the consumer's consent before the end of the seven-day period referred to in this section;

e. 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;

f. 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 likely to deteriorate or expire rapidly;

g. where audio or video recordings or computer software were downloaded or unsealed by the consumer;

h. for the sale of newspapers, periodicals, magazines and books;

i. for the provision of gaming and lottery services;

j. for online gambling;

k. 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; and

l. such other exception/s as may be prescribed.

Section 28: Applicability of foreign law

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

Section 29: Non-exclusion

Any provision in an agreement which excludes any rights provided for in this chapter is null and void.

CHAPTER 9: ONLINE MARKETING

Section 30: Unsolicited commercial communications

(1) 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(s);

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 will be 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 recipient with an operational opt-out facility referred to in subsections 1b and 3d is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8.

(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, is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8.

(7) Any party whose goods or services are advertised in contravention of this section is guilty of an offence and liable, on conviction, to the penalties prescribed in subsection 8.

(8) A person convicted of an offence referred to in this section is liable on conviction to a fine or imprisonment for a period not exceeding five years.

Part V

PART V: SERVICE PROVIDERS

CHAPTER 10: ONLINE SAFE HARBOURS

Section 31: Mere conduit

(1) A service provider shall not be subject to any civil liability in respect of third-party material in the form of electronic communications to which he merely provides access to information system services for the transmitting, routing or storage of electronic communications via an information system under its control, as long as 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 transmitting, routing and providing 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 recipients; and

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

Section 32: Caching

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 recipients of the service upon their request, as long as 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 by industry;

d. does not interfere with the lawful use of rights management information, widely recognized and used by 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 35.

Section 33: Hosting

(1) A service provider shall not be subject to 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 recipient of the service that consists of the storage of data provided by a recipient of the service, as long as 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; or

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 30, acts expeditiously to remove or to disable access to the data.

(2) The limitations on liability established by this section do 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 does not apply when the recipient of the service is acting under the authority or the control of the service provider.

Section 34: Information location tools

A service provider shall not be subject to 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 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 link of 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.

CHAPTER 11: REQUIREMENTS

Section 35: Take-down notification

(1) For the purposes of this chapter, a notification of unlawful activity shall be in the form of an electronic communication and it shall be addressed to 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;

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 a service provider knowing that it materially misrepresents the facts may be held liable for damages for wrongful take-down.

(4) A service provider is not liable for wrongful take-down in a bona fide response to a notification of unlawful activity which complies with subsection 2.

Section 36: No general obligation to monitor

(1) When providing the services contemplated in this chapter there is no general obligation on a service provider 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 recipients of their service; and

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

Section 37: Savings

(1) Sections 31-34 do not affect:

a. any obligation founded on an agreement;

b. the obligation of a service provider acting as such under a licensing or other regulatory regime established by or under any law;

c. any obligation imposed by law or by a court to remove, block or deny access to any electronic communication or to terminate or prevent unlawful activity in terms of any other law;

d. any additional right to limitation of liability based on the common law or the Constitution.

(2) This chapter does not affect the civil liability in terms of the common law or a statute.