Lesotho ELECTRONIC transactions AND ELECTRONIC COMMERCE BILL 2013

Act No. [ ] of [ ]

**ARRANGEMENT OF SECTIONS**

PART I 4

PRELIMINARY 4

Short title and commencement 4

Interpretation 4

Interpretation 7

Applicability 7

Variation by agreement 8

PART II 9

LEGAL RECOGNITION AND EFFECT OF ELECTRONIC COMMUNIACTIONS 9

Legal recognition of electronic communications 9

Writing 9

Electronic Signature 9

PART III 10

Electronic TRANSACTIONs 10

Formation and validity of contracts 10

Variation be agreement 10

Time of dispatch of electronic communications 10

Time of receipt of electronic communications 10

Time of contract formation 11

Automated transactions 11

Input errors 11

Part IV 13

Attribution 13

Original information 13

Admissibility and evidential weight of electronic communications 13

Retention of records 14

PART V 16

Regulation of certification authorities 16

Regulation of certification authorities 16

Recognition of foreign certification authorities 17

Regulation of repositories 17

Coming into force of Part V 17

Part VI 18

CRYPTOGRAPHY PROVIDERS 18

Register of cryptography providers 18

Registration compulsory 18

Restrictions on disclosure of information 18

Coming into force of Part VI 19

Application of Part and offences 19

PART VII 20

E-GOVERNMENT SERVICES 20

Acceptance of electronic filing and issuing of documents 20

Requirements may be specified 20

Procurement and use of information technology 20

PART VIII 22

CONSUMER PROTECTION 22

Scope of application 22

Suppliers’ obligations 22

Cooling-off period 23

Applicability of foreign law 23

Non-exclusion 24

Unsolicited electronic communications 24

Complaints to [to be specified] 24

PART IX 25

LIMITATION OF LIABILITY OF SERVICE PROVIDERS 25

Mere conduit 25

Caching 25

Hosting 25

Information location services 26

Take-down notification 26

No general obligation to monitor 27

Recognition of representative body 27

Conditions for eligibility 27

Savings 27

PART X 28

GENERAL PROVISIONS 28

Jurisdiction of courts 28

Offence by body corporate 28

Saving of common law 28

Power to exempt 28

Regulations 28

Limitation of liability 28

**Lesotho** ELECTRONIC transactions AND ELECTRONIC COMMERCE BILL 2013

#### Act No. [ ] of [ ]

**An Act to provide for the facilitation and regulation of electronic communications and transactions; to provide for protection of consumers and, to provide for the limitation of liability of service providers,; to encourage the use of e-government services; and for related matters.**

**ENACTED** by the Parliament of Lesotho

# PART I

# PRELIMINARY

## Short title and commencement

**1**. This Act may be cited as the Lesotho Electronic Transactions Act, [*a year of enactment*] and shall come into operation on such a date as the Minister may, by notice published in the *Gazette*, appoint.

## Interpretation

**2**. In this Act, unless the context otherwise requires -

“addressee” in respect 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;

“automated message system” means a pre-programmed system, or other automated system, used to: initiate an action; or 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.

 “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;

 “consumer” means any natural person and/or non-profit organization who enters or intends to entering into an electronic transaction with a supplier as the end user of the goods or service offered by that supplier;

 “cryptography provider” means any person who provides or who proposes to provide cryptography services *[or cryptography products]* in the Kingdom of Lesotho;

“cryptography service” means any service which is provided to a sender or a recipient of an electronic communication or to anyone storing an electronic communication, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring-

1. that such data or electronic communication can be accessed or can be put into an intelligible form only by certain persons;
2. that the authenticity or integrity of such data or electronic communication is capable of being ascertained;

*[provided that any references to the provision of cryptography services in this Act do not include the supply of, or of any right to use, computer software or computer hardware except where the supply is integral to the provision of cryptography services not consisting in such supply.]*

 “data message” means information generated, 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 and video recordings;

*[“Department” means the ICT Department established under Ministry of Communications, Science and Technology;]*

 “direct costs” means costs incurred as a result of transport costs or postage when returning goods or services but excludes any handling fees;

 *[“Director’’ means the Director of the Department;*]

 “e-government services” means any public service provided by electronic communications by any public office or any automated means intended for public service in the Kingdom of Lesotho;

“electronic communication” means a communication by means of data messages;

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

 “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;

“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;

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

“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;

**“**information system services**”** means providing a telecommunications system service including 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;

 “intermediary” with respect to a particular electronic communication, means a person who, on behalf of another person, whether as agent or not, sends, receives or stores that electronic communication or provides other services with respect to that electronic communication;

“Internet” means the interconnected system of networks that connects computers around the world using the TCP/IP and includes future versions thereof;

 “Minister” means the Minister of Communications, Science and Technology;

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

 “person” includes a natural and legal person;

 “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;

 “prescribe” means prescribe by regulation under this Act;

 “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;

“public body” means department or ministry of the Government, organ of State or statutory corporation;

 “relevant authorities” are authorities provided for and specified in this Act or any other person or a body as the Minister may appoint by notification in *Gazette* in relation to administration and enforcement of any issues governed by this Act and a “relevant authority” is any one of them;

“relevant subjects” are persons or entities regulated by relevant authorities;

“relevant parts of this Act” are Parts of this Act administered and enforced by relevant authorities;

 “rule of law” includes written law;

“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:

1. is unique to the signer for the purpose for which it is used;
2. can be used to identify objectively the signer of the electronic communication;
3. was created and affixed to the electronic communication by the signer or using a means under the sole control of the signer; and
4. 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.

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

“signed” or “signature” and its grammatical variations include any symbol executed or adopted, or any methodology or procedure employed or adopted, by a person with the intention of authenticating a record, including electronic or digital methods;

“telecommunications service” and “telecommunications system” have the same meaning as in the Lesotho Telecommunications Authority Act 2000, as amended.

 **Objects of the Act**

**3.** The purpose of this Act is to enable and facilitate electronic communications and transactions in the public interest, and for that purpose to -

1. recognize the importance of the information-economy and information-society for the economic and social prosperity of the Kingdom of Lesotho;
2. promote the understanding and, acceptance of and growth in the number of electronic transactions in the Kingdom of Lesotho;
3. remove and prevent barriers to electronic communications and transactions in the Kingdom of Lesotho resulting from uncertainties over writing and signature requirements;
4. promote legal certainty and confidence in the integrity and reliability of electronic communications and electronic commerce, and to foster the development of electronic commerce through the use of electronic signatures to lend authenticity and integrity to correspondence in any electronic medium;
5. promote the development of the legal and business infrastructure necessary to implement secure electronic commerce;
6. promote technology neutrality in the application of legislation to electronic communications and transactions;
7. promote e-government services and electronic communications and transactions with public and private bodies, institutions and citizens;
8. ensure that electronic transactions in the Kingdom of Lesotho conform to the highest international standards;
9. encourage investment and innovation in respect of electronic transactions in the Kingdom of Lesotho;
10. develop a safe, secure and effective environment for the consumer, business and the Government to conduct and use electronic transactions;
11. promote the development of electronic transactions services which are responsive to the needs of users and consumers; and
12. ensure compliance with accepted international technical standards in the provision and development of electronic communications and transactions.

## Interpretation

**4.** (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 Act 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.

(3) This Act shall apply to the law in force in the Kingdom of Lesotho.

## Applicability

**5**. (1) This Act 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 (2).

(2) Parts II and III shall not apply to any rule of law requiring writing or signatures in any of the following matters:

1. the creation or execution of a will;
2. negotiable instruments;
3. the creation, performance or enforcement of an indenture, declaration of trust or power of attorney with the exception of constructive and resulting trusts;
4. any contract for the sale or other disposition of immovable property, or any interest in such property;
5. the conveyance of immovable property or the transfer of any interest in immovable property;
6. documents of title.

(3) Nothing in this Act shall be construed as:

1. requiring any person to use or to accept electronic communications; or
2. 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.

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

(5) The Minister may by order modify the provisions of subsection (2) by adding, deleting or amending any class of transactions or matters.

## Variation by agreement

**6.** (1) As between the parties involved in generating, sending, receiving, storing or otherwise processing electronic communications, and except as otherwise provided, sections 8 and 9 and/or the provisions of Part III may be varied by agreement.

(2) Subsection (1) does not effect any right that may exist to modify by agreement any rule of law referred to in Part II.

# PART II

# LEGAL RECOGNITION AND EFFECT OF ELECTRONIC COMMUNIACTIONS

## Legal recognition of electronic communications

**7.** (1) A data message shall not be denied legal effect, validity or enforceability solely on the ground that it is wholly or partly in the form of an electronic communication.

(2) 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.

(3) Information shall not be denied legal force and effect merely on the grounds 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 such electronic communication.

## Writing

**8**.(1) Where a rule of law requires information to be in writing or provides for certain consequences if it is not, an electronic communication satisfies that rule of law 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.

## Electronic Signature

## 9. (1) Where a law requires the signature (manuscript) of a person, that requirement is met by a secure electronic signature.

(2) Subject to subsection (1) an electronic signature shall not be denied legal force merely on the grounds that it is in electronic form

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

1. the method is used to identify the person and to indicate the person’s intention in regard to the information communicated; and
2. 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

# PART III

# Electronic TRANSACTIONs

## Formation and validity of contracts

**10**.(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.

## Variation by agreement

**11**. The provisions under Part III shall apply, unless the parties involved in generating, sending, receiving, storing or otherwise processing electronic communications, have agreed otherwise.

## Time of dispatch of electronic communications

**12**. —(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.

## Time of receipt of electronic communications

**13**. (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:

1. at the time when the electronic communication enters the designated information system; or
2. 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.

**Place of dispatch and receipt of electronic communications**

**14** (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:

1. if the originator or the addressee has more than one place of business, the place of business is:
	1. 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,
	2. if there is no underlying transaction, the principal place of business.
2. If the originator or the addressee does not have a place of business, reference is to be made to the that person’s habitual place of residence; and
3. The “usual place of residence”, in relation to a body corporate, means the place where it is incorporated or otherwise legally constituted.

(6) 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..

## Time of contract formation

**15**. (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.

## Automated transactions

**16.** (1) A contract formed by the interaction of an automated message system and a natural person, or by the interaction of automated message systems, shall not be denied 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.

## Input errors

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

1. 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;
2. 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;
3. 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;
4. 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.

(2) Nothing in this section 17 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 (1).

# Part IV

ELECTRONIC COMMERCE

## Attribution

**18**. (1) An electronic communication is that of the originator if it was sent by:

1. the originator himself.
2. by a person who had the authority to act on behalf of the originator in respect of that electronic communication; or
3. by an information system programmed by or on behalf of the originator to operate automatically.

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

## Original information

**19**. (1) Where the law requires information to be presented or retained 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.

## Admissibility and evidential weight of electronic communications

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

1. on the sole grounds that it is constituted by an electronic communication; or
2. 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 must be given due evidential weight.

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

1. the reliability of the manner in which the electronic communication was generated, stored or communicated;
2. the reliability of the manner in which the integrity of the electronic communication was maintained;
3. the manner in which its originator was identified; and
4. 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:

1. the affidavit is made by the person who was in control of the system at the time when the electronic communication was created;
2. 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.

## Retention of records

**21**.(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:

1. the electronic record contained therein is an electronic communication;
2. 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
3. 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) shall 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 the conditions set forth in paragraphs (a) to (c) of subsection (1) are met.

**Production of document or information**

1. (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:
2. 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
3. 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

1. the addition of any endorsement; or
2. any immaterial change, which arises in the normal course of communication, storage or display.

**Notarisation, acknowledgement and certification**

1. (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

Other requirements

1. (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 V

# Regulation of certification authorities

## Regulation of certification authorities

## 25 (1) The Minister may make regulations for the regulation and licensing of certification authorities and to define when an authentication product qualifies as a secure electronic signature.

(2) Without prejudice to the generality of subsection (1), the Minister may make regulations for or with respect to:

1. the technical requirements that an authentication product must meet; be it based on asymmetric crypto system; biometrics or a combination of these or other authentication methods to qualify as secure electronic signatures;
2. applications for licences or renewal of licences of certification authorities and their authorised representatives and matters incidental thereto;
3. the activities of certification authorities including the manner, method and place of soliciting business, the conduct of such solicitation and the prohibition of such solicitation of members of the public by certification authorities which are not licensed;
4. the standards to be maintained by certification authorities;
5. prescribing the appropriate standards with respect to the qualifications, experience and training of applicants for any licence or their employees;
6. prescribing the conditions for the conduct of business by a certification authority;
7. providing for the content and distribution of written, printed or visual material and advertisements that may be distributed or used by a person in respect of a digital certificate or key;
8. prescribing the form and content of a digital certificate or key;
9. prescribing the particulars to be recorded in, or in respect of, accounts kept by certification authorities;
10. providing for the appointment and remuneration of an auditor appointed under the regulations and for the costs of an audit carried out under the regulations;
11. providing for the establishment and regulation of any electronic system by a certification authority, whether by itself or in conjunction with other certification authorities, and for the imposition and variation of such requirements, conditions or restrictions as may be applicable;
12. the manner in which a holder of a licence conducts its dealings with its customers, conflicts of interest involving the holder of a licence and its customers, and the duties of a holder of a licence to its customers with respect to digital certificates;
13. the recommended reliance limits certification authorities may specify;
14. the limitation of liability of licensed certification authorities for any loss caused by reliance on a false or forged secure electronic signature;
15. the quality of repositories and the services they provide including provisions for the standards, licensing or accreditation of repositories
16. prescribing forms for the purposes of the regulations;
17. prescribing fees to be paid in respect of any matter or thing required for the purposes of this Act or the regulations; and
18. any other matter deemed to be necessary for the efficient functioning of the matters addressed in the Part.

(3) Regulations made under this section may provide that a contravention of a specified provision shall be an offence and may provide penalties not exceeding a fine of *[to be specified]* or imprisonment for a term not exceeding *[to be specified]* months or both.

## Recognition of foreign certification authorities

**26.** The Minister may, by regulations, recognise certification authorities outside Kingdom of Lesotho that satisfy the prescribed requirements for any of the following purposes:

1. the recommended reliance limit, if any, specified in a digital certificate issued by the certification authority;
2. the presumptions referred to in section 18.

## 27. Coming into force of Part V

 This Part V shall come into force on such day as the Minister may by order made by statutory instrument appoint; and different days may be appointed under this subsection for different purposes.

# Part VI

# CRYPTOGRAPHY PROVIDERS

## Register of cryptography providers

**28.** (1) The Minister must establish and maintain a register of cryptography providers who are for the time being approved under arrangements in force under this section.

(2)The Minister must record the following particulars in respect of a cryptography provider in that register:

1. the name and address of the cryptography provider;
2. a description of the type of cryptography service *[or cryptography product]* being provided; and
3. such particulars as may be prescribed to identify and locate the cryptography provider or its product or services adequately.
4. the conditions of the approval.

(3) A cryptography provider is not required to disclose confidential information or trade secrets in respect of its cryptography products or services.

## Registration compulsory

## 29. (1) No person may provide cryptography services or cryptography products in the Kingdom of Lesotho until the particulars refers to in section 28 in respect of that person have been recorded in the register contemplated in section 28.

(2) A cryptography provider must in the prescribed manner furnish the Minister with the information required and pay the prescribed administrative fee.

(3) A cryptography service or cryptography product is regarded as being provide in the Kingdom of Lesotho if it is provided:-

(a) from premises in Lesotho:

(b) to a person who is present in the Republic when that person makes use of the service or product: or

(c) to a person who uses the service or product for the purpose of a business carried on in the Lesotho or from premises in Lesotho..

## Restrictions on disclosure of information

**30**. (1) Information contained in the register provided for in section 29 must not be disclosed to any person other than to employee of the Department who are responsible for the keeping of the register.

(2) Subsection 1 does not apply in respect of information which is disclosed:-

1. to a relevant authority which investigates a criminal offence or for the purposes of any criminal proceedings;
2. to government agencies responsible for safety and security in the republic pursuant to an official request;
3. to a cyber inspector; or
4. for the purpose of any civil proceedings which relate to the provision of cryptography services or cryptography products and to which a cryptography provider is a party.

## Coming into force of Part VI

**31**. This Part VI shall come into force on such day as the Minister may by order made by statutory instrument appoint; and different days may be appointed under this Part for different purposes.

## Application of Part and offences

**32**. (1) The provisions of this Part VI do not apply to the [*national intelligence agencies and similar institutions*].

(2) A person who contravenes or fails to comply with a provision of this Part VI is guilty of an offence and liable on conviction to *[a fine or to imprisonment for a period not exceeding [ ] years*].

# PART VII

# E-GOVERNMENT SERVICES

## Acceptance of electronic filing and issuing of documents

**33.** Any public body that, pursuant to any law-

1. accepts the filing of documents, or requires that documents be created or retained:
2. issues any permit, licence or approval; or
3. provides for a manner of payment,

 may, notwithstanding anything to the contrary in such law -

 (i) accept the filing of such documents, or the creation or retention of such documents in the form of electronic communications;

 (ii) issue such permit, licence or approval in the form of an electronic communication; or

 (iii) make or receive payment in electronic form or by electronic means.

## Requirements may be specified

**34.** (1) In any case where a public body performs any of the functions referred to in section 33, such body may specify by [notice in the *Gazette*]*-*

1. the manner and format in which the electronic communications must be filed, created, retained or issued;
2. in cases where the electronic communication has to be signed, the type of electronic signature required (including, if applicable, a requirement that the sender use a digital signature or other secure electronic signature);
3. the identity of or criteria that must be met by any certification authority used by the person filing the document [or that or that such certification authority must be a preferred certification authority designated in accordance with subsection (2)];
4. the appropriate control processes and procedures to ensure adequate integrity, security and confidentiality of electronic communications or payments; and
5. any other requirements for electronic communications or payments.

[(2) For the purposes of subsection (1)(d) the Minister may designate a certification authority as a preferred certification authority.]

(3) Nothing in this Act shall by itself compel any public body to accept or issue any document in the form or electronic communications.

## Procurement and use of information technology

**35** (1) For the purpose of this section, “procurement” includes but is not limited to acquisition, purchase, procurement, hire, outsourcing, disposal or transfer.

(2) *[The Minister ] [Director]* shall exercise control over the use or procurement of all telecommunications and information technology equipment and services by any public body. [In exercising its power under this section, the *[The Minister] [Director]* may:

1. prescribe guidelines or make regulations regarding the use of any telecommunications and information technology equipment or services by a public body;
2. prescribe guidelines or make regulations regarding safety and security of telecommunications and information technology equipment or services used by a public body;
3. oversee any use of any telecommunications and information technology equipment or services by a public body;
4. *[The Minister] [Director]* can direct any public body or any officer or employee thereof to take such measures or stop carrying on such activities as are specified in the notice if they are necessary to ensure compliance with the provisions of this Act or any regulations made thereunder;

PART VIII

#  CONSUMER PROTECTION

## Scope of application

**36.** (1) This Part applies only to contracts concerning goods or services concluded between a supplier and a consumer by means of electronic communications.

(2) Section 39 does not apply to contracts -

1. for financial services, including but not limited to, investment services, insurance and reinsurance operations, banking services and operations relating to dealings in securities;
2. by way of an auction;
3. for the supply of foodstuffs, beverages or other goods intended for everyday consumption supplied to the home, residence or workplace of the consumer;
4. for services which began with the consumer’s consent before the end of the seven-day period referred to in section 39;
5. 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;
6. 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;

1. where audio or video recordings or computer software were downloaded or unsealed by the consumer;
2. for the sale of newspapers, periodicals, magazines and books;
3. for the provision of gaming and lottery services;
4. for on-line gambling; or
5. 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.

## Suppliers’ obligations

**37.** (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:

1. its full contact details, including its place of business, e-mail addresses and telefax number(s);
2. 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;
3. the full price of the goods or services, including transport costs, taxes and any other fees or costs;
4. 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;
5. 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: –

1. to review the entire electronic transaction;
2. to correct any mistakes; and
3. 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: –

1. the consumer shall return the performance of the supplier or, where applicable, cease using the services performed; and
2. the supplier shall refund all payments made by the consumer minus the direct cost of returning the goods.

**Performance**

**38** (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.

## Cooling-off period

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

1. of goods within seven days after the date of the receipt of the goods; or
2. of services within seven days after the date of the conclusion of the contract.

(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 refund must be made within 30 days of the date of cancellation.

(4) This section must not be construed as prejudicing the rights of a consumer provided for in any other law.

## Applicability of foreign law

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

## Non-exclusion

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

## Unsolicited electronic communications

**42.** (1) Marketing by means of electronic communication shall provide the addressee with:

1. the originator’s identity and contact details including its place of business, e-mail, addresses and telefax number(s);
2. a valid and operational opt-out facility from receiving similar communications in future; and
3. 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:

1. 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”;
2. the originator only sends promotional messages relating to its “similar products and services” to the addressee;
3. 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
4. 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.

## Complaints to [to be specified]

**43.** The Minister shall by regulation prescribe procedures by which **a** consumer may lodge a complaint with the *[to be specified]* in respect of any non-compliance with the provisions of this Part by a supplier.

# PART IX

# LIMITATION OF LIABILITY OF SERVICE PROVIDERS

## Mere conduit

**44.** (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 a telecommunications system for the transmission in a telecommunications system of information provided by a recipient of a telecommunications service, routing or storage of electronic communications via an information system under its control, as long as the service provider:

1. did not initiate the transmission;
2. does not select the receiver of the transmission;
3. did not select or modify the information 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:

1. for the sole purpose of carrying out the transmission in the telecommunications system;
2. in a manner that makes it ordinarily inaccessible to anyone other than anticipated recipients; and
3. for a period no longer than is reasonably necessary for the transmission.

## Caching

**45** 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:

1. does not modify the information;
2. complies with conditions on access to the data;
3. complies with any rules regarding the updating of the data,, specified in a manner widely recognised and used by industry;
4. does not interfere with the lawful use of rights management information, widely recognised and used by industry, to obtain information on the use of the data; and
5. removes or disables access to the data it has stored upon receiving a take-down notification referred to in section 49.

## Hosting

**46.** 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:

1. 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
2. is not aware of facts or circumstances from which the infringing activity or the infringing nature of the electronic communication is apparent; and
3. upon receipt of a take-down notification from the aggrieved party referred to in section 49, 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.

## Information location services

**47** 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:

1. does not have actual knowledge that the electronic communication or an activity relating to the electronic communication is infringing the rights of that person;
2. is not aware of facts or circumstances which evidences the infringing activity or the infringing nature of the electronic communication;
3. does not receive a financial benefit directly attributable to the infringing activity; and
4. 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.

## Take-down notification

**48**. (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:

1. the full names and address of the complainant;
2. the signature of the complainant;
3. identification of the right that has allegedly been infringed;
4. identification of the material or activity that is claimed to be the subject of unlawful activity;
5. the remedial action required to be taken by the service provider in respect of the complaint;
6. telephonic and electronic contact details, if any, of the complainant;
7. a statement that the complainant is acting in good faith;
8. 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.

##

## No general obligation to monitor

**49.** (1) When providing the services contemplated in this Part there is no general obligation on a service provider to:

1. monitor the data which it transmits or stores; or
2. actively seek facts or circumstances indicating an unlawful activity.

(2) The Minister may issue regulations prescribing procedures for service providers to:

1. inform the competent public authorities of alleged illegal activities under-taken or information provided by recipients of their service; and
2. to communicate to the competent authorities, at their request, information enabling the identification of recipients of their service.

## Recognition of representative body

## 50 (1) The Minister may, on application by an industry representative body for service providers by notice in the Gazette, recognize such body for purposes of this Act

(2) The Minister may only recognize a representative body referred to in subsection (1) if the Minister is satisfied that:-

1. its members are subject to a code of conduct;
2. membership is subject to adequate criteria;
3. the code of conduct requires continued adherence to adequate standards of conduct; and
4. the representative body is capable of monitoring and enforcing its code of conduct adequately.

## Conditions for eligibility

## 51. The limitations on liability established by this Part apply to a service provider only if:

(a) the service provider is a member of representative body referred to in this Act and

(b) the service provider has adopted and implemented the official code of conduct of that representative body.

## Savings

**52.**  This Part does not affect-

1. any obligation founded on an agreement;
2. the obligation of a service provider acting as such under a licensing or other regulatory regime established by or under any law;
3. any obligation imposed by law or by a court to remove, block or deny access to any information; or
4. any right to limitation of liability based on the common law or the Constitution.

# PART X

# GENERAL PROVISIONS

## Offence by body corporate

**53**. Where an offence under this Act or any regulations made thereunder is committed by a body corporate, and it is proved to have been committed with the consent or connivance of, or to be attributable to any act or default on the part of, any director, manager, or similar officer of the body corporate, or any person who was purporting to act in any such capacity, he, as well as the body corporate, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

## Saving of common law

**54.**  This Act does not affect criminal or civil liability in terms of the common law.

## Power to exempt

**55.** The Minister may exempt, subject to such terms and conditions as he thinks fit, any person or class of persons from all or any of the provisions of this Act or any regulations made thereunder.

## Regulations

**55**. The Minister may make regulations to prescribe anything, which is required to be prescribed under this Act and generally for the carrying out of the provisions of this Act.

## Limitation of liability

**56.** Neither the State, the Minister, nor any employee of the State is liable in respect of any act or omission in good faith and without gross negligence in performing a function in terms of this Act.