Print

ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT

Arrangement of Sections

Section

PART I
PRELIMINARY

1. Short title
2. Interpretation
3. Application

PART II
LEGAL REQUIREMENTS FOR DATA MESSAGES

4. Legal requirements for data messages
5. Writing
6. Use of advanced electronic signature
7. Determination of originality of data message
8. Admissibility and evidential weight of data messages
9. Retention of information in data message
10. Production of document or information
11. Notarisation, acknowledgment and certification
12. Other requirements
13. Automated transactions

PART III
COMMUNICATION OF DATA MESSAGES

14. Variation by agreement between parties
15. Formation and validity of agreements
16. Time and place of communication, dispatch and receipts

17. Expression of intent or other statement

18. Attribution of data messages to originator

19. Acknowledgment of receipt of data message

20. Acceptance of electronic filing and issuing of documents

21. Requirements may be specified

PART IV
CRYPTOGRAPHY PROVIDERS

22. Registration to provide cryptograph services or products

23. Register of cryptography providers

24. Restrictions on disclosure of information in Register

PART V
ACCREDITATION AND RECOGNITION OF AUTHENTICATION SERVICE PROVIDERS

25. Definition

26. Appointment of Accreditation Authority and other officers

27. Selling of authentication products or services

28. Powers and duties of Accreditation Authority

29. Accreditation of authentication products and services

30. Criteria for accreditation

31. Revocation or suspension of accreditation

32. Recognition of accredited foreign products and services

33. Accreditation regulations

PART VI
CONSUMER PROTECTION

34. Scope of application

35. Information to be provided by supplier

36. Cooling off period

37. Performance

38. Applicability of foreign law

39. Non exclusion

40. Complaints to Authority

PART VII
PROTECTION OF PERSONAL INFORMATION

41. Scope of protection of personal information

42. Principles for electronically collecting personal information

PART VIII
PROTECTION OF CRITICAL DATABASES

43. Scope of critical database protection

44. Identification of critical data and critical databases

45. Registration of critical databases

46. Management of critical databases

47. Restrictions on disclosure of information

48. Audit of critical database

49. Non compliance with Part

PART IX
DOMAIN NAME REGULATION

50. Regulation of domain name

51. Licensing of Registrars and registries

52. Regulations regarding registeries, etc

53. Dispute resolution

PART X
LIMITATION OF LIABILITY OF SERVICE PROVIDERS

54. Definition

55. Recognition of representative body for service provider

56. Conditions for eligibility of service provider

57. No liability for mere conduit

^
(/)

58. Caching

59. Hosting

60. Use of information location tools by service provider

61. Take down notification

62. No general obligation on service provider to monitor unlawful activities

63. Savings

PART XI

INTERCEPTION OF COMMUNICATION

64. Prohibition of interception of communication

65. Central Monitoring and Coordination Centre

66. Power to intercept communication and admissibility of intercepted communication

67. Interception of communication to prevent bodily harm, loss of life or damage to property

68. Interception of communication for purposes of determining location in case of emergency

69. Prohibition of disclosure of intercepted communication

70. Disclosure, etc. of intercepted communication by law enforcement officer

71. Privileged communication to retain privileged character

72. Prohibition of random monitoring

73. Protection of user, etc. from fraudulent or other unlawful use of service

74. Disclosure of communication inadvertently obtained by service provider

75. Interception of satellite transmission

76. Prohibition of use of interception device

77. Assistance by service providers

78. Duties of service provider in relation to customers

79. Interception capability of service provider

PART XII

ACCESS TO STORED COMMUNICATION

80. Prohibition of disclosure of stored communication

81. Disclosure of customer records

82. Access to communication in electronic storage

83. Access to communication in remote computing service

84. Access to record of electronic communication service or remote computing service

PART XIII
ENCRYPTING COMMUNICATION

85. Use of encrypted communication

86. General construction

87. Prohibition of unauthorised decryption or release of decryption key

88. Prohibition of disclosure of record or other information by key holder

89. Obstruction of law enforcement officer

90. Sale and acquisition of encryption products

91. Prohibition of disclosure or use of stored recovery information

92. Immunity of recovery agents

PART XIV
CYBER INSPECTIONS

93. Appointment of cyber inspectors

94. Powers of cyber inspectors

95. Power to inspect, search and seize

96. Warrant entering, etc

97. Prohibition of disclosure of information to authorised persons

PART XV
CYBER CRIME

98. Definition

99. Unauthorised access to, interception of or interference with data

100. Computer related extortion, fraud and forgery

101. Attempt, aiding and abetting

102. Prohibition of pornography

103. Hacking, cracking and introduction of viruses, etc. into computer system

104. Denial of service attacks

105. Spamming

106. Prohibition of illegal trade and commerce

107. Application of offences under this Act

108. Offence committed by body corporate or un-incorporate body

109. Cognizable offences

PART XVI
GENERAL PROVISIONS

110. General penalty

111. Evidence obtained by unlawful interception not admissible in criminal proceedings

112. Data protection by Investigator-General

113. Regulations

114. Repeal of Act 13 of 2004

AN ACT

to develop a safe, secure and effective environment for the consumer, business sector and the Government to conduct and use electronic communications; promote legal certainty and confidence, and encourage investment and innovation, in the electronic communications industry; facilitate the creation of secure communication systems and networks; establish the Central Monitoring and Coordination Centre and define its functions; repeal the Computer Misuse and Crimes Act, 2004; and provide for matters connected with or incidental to the foregoing.

[*4th December, 2009*]

Act 21 of 2009,

SI 105 of 2009,

PART I
PRELIMINARY

1. Short title

This Act may be cited as the Electronic Communications and Transactions Act.

2. Interpretation

In this Act, unless the context otherwise requires—

"access" in relation to a computer system or electronic communication system, means the right to use or open the whole or any part of the computer system or electronic communication system, or to see, open, use, get or enter information in the computer system or electronic communication system, with authorisation from the owner or operator thereof;

"addressee" in relation to a data message, means a person who is intended by the originator of the data message to receive it, but not a person acting as an intermediary in respect of that data message;

"advanced electronic signature" means an electronic signature that is unique to the user, capable of verification, under the sole control of the person using it, and linked to the data in such a manner that if the data is changed, the signature is invalidated;

"Anti-Corruption Commission" means the Anti-Corruption Commission established under the Anti-Corruption Commission Act;

"aural transfer" means a transfer containing the human voice at a point between, and including, the point of origin and the point of reception;

"authentication products or services" means products or services designed to identify the holder of an electronic signature to other persons;

"authentication service provider" means a person whose authentication products or services are accredited by the Accreditation Authority under section 29 or recognised by the Minister under section 32;

"Authority" means the Communications Authority continued under section 4 of the Information and Communication Technologies Act, 2009;

"automated transaction" means an electronic transaction conducted or performed, in whole or in part, by means of data messages in which the conduct of data messages of one or both parties are not reviewed by a natural person in the ordinary course of the natural person's business or employment;

"browser" means a computer program which allows a person to read a hyperlinked data message;

"cache" means high speed memory that stores data for relatively short periods of time, under computer control, in order to speedup data transmission or processing;

"call-related information" includes switching, dialing or signaling information that identifies the origin, destination, termination, duration and equipment identification of each communication generated or

received by a customer or user of any equipment, facility or service provided by a service provider and, where applicable, the location of the user within the telecommunications system;

"ccTLD" means country code domain at the top level of the internet's main system signed according to the two-letter codes in the International Standard ISO 3166-1, Codes for Representation of Names of Countries and their Subdivision;

"certification service provider" means a person providing an authentication product or service in the form of a digital certificate attached to, incorporated in or logically associated with, a data message;

"communication" means oral, wire or electronic communication;

"computer" means an electronic, magnetic, optical, electrochemical or other high speed data processing device, performing logical, arithmetic or storage functions, of any data storage facility or communications facility directly related to, or operating in conjunction with, such device;

"computer data" means a representation of facts, information or concepts in a form suitable for processing in a computer system, or a program which is able to cause a computer system to perform a function;

"computer system" means a device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

"computer virus" means a written software which is willfully spread for purposes of causing damage to a computer system;

"consumer" means any natural person who enters, or intends to enter, into an electronic message with a supplier as the end-user of the goods or services offered by that supplier;

"content" in relation to an electronic communication, includes any information concerning the substance, purport or meaning of that communication;

"cracking" means an illegal act of decoding a password;

"critical data" means data that is declared by the Minister under section 44 to be important for purposes of national security or the economic and social well-being of the citizens of Zambia;

"critical database" means a collection of critical data in electronic form from where it may be accessed, reproduced or extracted;

"critical database administrator" means the person responsible for the management and control of a critical database;

"cryptograph product" means any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring—

(*a*) that such data can be accessed only by relevant persons;

(*b*) the authenticity of the data;

(*c*) the integrity of the data; or

(*d*) that the source of the data can be correctly ascertained;

"cryptography provider" means a person who provides, or who proposes to provide, cryptograph services or products in Zambia;

"cryptograph service" means any service which is provided to a sender or a recipient of a data message, or to anyone storing a data message, and which is designed to facilitate the use of cryptographic techniques for the purpose of ensuring—

(*a*) that such data or data message can be accessed, or can be put, into an intelligible form only by certain persons;

(*b*) that the authenticity or integrity of such data or data message is capable of being ascertained;

(*c*) the integrity of the data or data message; or

(*d*) that the source of the data or data message can be correctly ascertained;

"cyber" means the use, simulated environment or state of connection or association with electronic communications or networks including the internet;

"cyber inspector" means a person appointed as such under section 93;

"damage" means an impairment to the integrity or availability of data, a program, a system or information;

"data" means electronic representations of information in any form;

"data controller" means any person, either alone or in common with other persons, who controls and is responsible for keeping and using of personal information on a computer, or in structured manual files, and electronically requests, collects, collates, processes or stores personal information from or in respect of a data subject;

"data interference" means the corruption, damaging, deletion, deterioration, alteration or suppression of computer data without authority;

"data message" means data generated, sent, received or stored by electronic means and includes—

(*a*) a voice, where the voice is used in an automated transaction; and

(*b*) a stored record;

"data subject" means any natural person from, or in respect of whom, personal information has been requested, collected, collated, processed or stored, after the commencement of this Act;

"decryption" means the electronic transformation of data or communication that has been encrypted;

"delayed access message service" means a method by which a communication intended for a person can be submitted using a communications system, without the person being in direct contact with anyone submitting the communication and can be subsequently accessed by the person, whether or not other persons are able to access it;

"denial" of service attacks means rendering a computer system incapable of providing normal services to its legitimate users;

"device" means an apparatus which can be used to intercept a wire, oral or electronic communication other than—

(*a*) a telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of business and—

(i) used by the subscriber or user in the ordinary course of business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of business; or

(ii) used by a provider of wire or electronic communication service in the ordinary course of business, or by a law enforcement officer in the ordinary course of the law enforcement officer's duties; or

(*b*) a hearing aid or similar device;

"digital signature" means an electronic signature consisting of a transformation of an electronic record using an asymmetric crypto-system such that a person having the initial untransformed electronic record and the signer's public key can accurately be determined—

(*a*) whether the transformation was created using the private key that corresponds to the signer's public key; or

(*b*) whether the initial electronic record has been altered since the transformation was made; and includes voice recognition features, digital fingerprinting or such other biotechnology feature or process, as may be prescribed;

"distributed denial of service" means an attack that makes use of the user or server technology to multiply the effectiveness of the denial of service attack on one or more computer systems;

"domain name" means an alpha-numeric designation that is registered or assigned in respect of an electronic address or other resource on the internet;

"domain name system" means a system to translate domain names into IP address or other information;

(*l*)

"Drug Enforcement Commission" means the Drug Enforcement Commission established under the

Narcotic Drugs and Psychotropic Substances Act;

"e-government service" means any public service provided by electronic means by any public body;

"electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to data messages or performances in whole or in part, in an automated transaction;

"electronic signature" means data attached to, incorporated in, or logically associated with other data and which is intended by the user to serve as a signature; electronic communication means a transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by radio, electromagnetic, photo-electronic or photo-optical system, but does not include—

(*a*) any wire or direct oral communication;

(*b*) any communication made through a tone-only paging device;

(*c*) any communication from a tracking device; or

(*d*) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

"electronic communications system" means a radio, electromagnetic, photo-optical or photo-electronic facility for the transmission of electronic communications, and any computer facility or related electronic equipment, for electronic storage of such communications;

"electronic communication service" means any service which provides the ability to send or receive electronic communications to users;

"electronic storage" means—

(*a*) a temporary or intermediate storage of an electronic communication incidental to the electronic transmission thereof; and

(*b*) a storage of any communication by an electronic communication service for purposes of backup for protection of such communication;

"electronic surveillance" means—

(*a*) the installation or use of an electronic, mechanical or other surveillance device for acquiring information, by intentionally directing surveillance at a particular known person who is located within Zambia under circumstances in which that person has a reasonable expectation of privacy; or

(*b*) the intentional acquisition of the contents of any communication under circumstances in which a person has a reasonable expectation of privacy;

electronic user means a known person who is expected to possess control transmit or receive electronic information while the person is within Zambia; (*l*)

"e-mail" means electronic mail or a data message used, or intended to be used, as a mail message between the originator and addressee in an electronic communication;

"encryption" means the electronic transformation of data in order to obscure or hide its content;

"hacking" means to access a computer illegally from a remote location, or without the authority of the owner;

"home page" means the primary entry point web page of a website;

"hyperlink" means a reference or link from some point in one data message or other technology or functionality, directing a browser or other technology or functionality, to another data message or point therein or to another place in the same data message;

"ICANN" means the Internet Corporation for Assigned Names and Numbers, a California non-profit public benefit corporation established under the laws of the State of California in the United States of America;

"illegal trade and commerce" means any internet fraud- related activity, or the use of the internet as a medium for illegal trade or any other illegal activity;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages, and includes the internet;

"information system services" includes the provision of connections, the operation of facilities for information systems, the provision of access to information systems, the transmission or routing of data messages between or among points specified by a user and the processing and storage of data, at the request of the recipient of the service;

"infringement" means the illegal use of copyright and other intellectual property rights;

"intelligence" means—

(*a*) information, whether or not concerning an electronic user within or outside Zambia, that relates to the ability of the Republic of Zambia to protect against—

(i) an actual or potential breach, attack or any grave or hostile act on a wire or electronic communication system;

(ii) any breach, sabotage or terrorism on a wire or electronic communication system by a person within or outside Zambia, a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service, a network of a foreign power or an agent of a foreign power;

(*b*) information, whether or not concerning a citizen of Zambia or an electronic user with respect to a foreign power or foreign territory, that relates to the national defence or the security of the Republic of Zambia; or

(*l*)

(*c*) the conduct of the foreign affairs of Zambia;

"intercept" means to access or acquire the contents of a communication through an electronic, mechanical or other device;

"interception device" means a device or process which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached;

"intermediary" means a person who, on behalf of another person, whether as agent or not, sends, receives or stores a particular data message or provides other services with respect to that data message;

"internet" means the interconnected system of networks that connects computers around the world using the TCP/ IP or other protocols, and includes future versions thereof;

"IP address" means the dynamic or static number identifying the point of connection of a computer or other device to the internet;

"judge" means a judge of the High Court;

"law enforcement officer" means—

(*a*) a police officer above the rank of sub-inspector;

(*b*) an officer of the Anti-Corruption Commission;

(*c*) an officer of the Drug Enforcement Commission;

(*d*) an officer of the Zambia Security Intelligence Service; and

(*e*) any other person appointed as such by the Minister for purposes of this Act;

"misuse of device" means the production, sale, procurement for use, distribution, possession or otherwise making available, of a computer password, access code or data by which the whole or any part of a computer system is capable of being accessed, or a device or computer program designed or adapted primarily for the purpose of committing an offence;

"Monitoring Centre" means the Central Monitoring and Coordination Center established pursuant to section 65;

"natural person" means an individual;

"oral communication" means a verbal communication or any communication through sign language, but does not include any electronic communication;

"originator" means a person by whom, or on whose behalf, a data message 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 data message;

"person" includes a public body;

"personal information" means information about an identifiable individual, including, but not limited to—

(*a*) information relating to the race, gender, pregnancy, marital status, nationality, ethnic or social origin, colour, age, physical or mental health, well-being, disability, religion, belief, culture, language and birth of the individual;

(*b*) information relating to the education or the medical, criminal or employment history of the individual, or information relating to financial transactions in which the individual has been involved;

(*c*) any identifying number, symbol, or other particular assigned to the individual;

(*d*) the address, fingerprints or blood type of the individual;

(*e*) the personal opinions, views or preferences of the individual, except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual;

(*f*) correspondence sent by the individual that is implicitly or explicitly of a private or confidential nature, or further correspondence that would reveal the contents of the original correspondence;

(*g*) the views or opinions of another individual about the individual;

(*h*) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual, but excluding the name of the other individual where it appears with the views or opinions of the other individual; and

(*i*) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but excludes information about an individual who has been dead for more than twenty years;

"private body" means—

(*a*) a natural person who carries, or has carried on, any trade, business or profession, but only in such capacity;

(*b*) a partnership which carries, or has carried on, any trade, business or profession; or

(*c*) any former or existing juristic person, other than a public body;

"plain text" means decrypted or unencrypted data;

"pornography" means material that visually depicts images of a person engaged in explicit sexual conduct;

"public body" means—

(*a*) any department of the Government or any local authority; or

(*l*)

(*b*) any other functionary or institution exorcising—

(i) a power, or performing a duty, under the Constitution; or

(ii) a power, or performing a function, under any other law;

"recovery agent" means a person or entity who provides recovery information for storage services;

"recovery device" means hardware or software, that allows plaintext to be obtained, even if attempts are made to protect it through encryption or other security techniques or devices, by enabling a modification of any part of a computer or other system;

"recovery information" means a parameter that can he used with an algorithm, other data or object, which can be used to decrypt data or communications;

"registrant" means an applicant for, or holder of, a domain name;

"Registrar" means an entity which is licensed by the Authority to update a repository;

"Register" means the Register of cryptography providers established under section 22;

"registry" means an entity licensed by the Authority to manage and administer a specific sub-domain;

"remote computing service" means the provision of computer storage or processing services to the public by means of an electronic communications system;

"second level domain" means the sub-domain immediately following the ccTLD;

"service provider" means a public or private entity authorised to—

(*a*) provide or offer electronic communications by means of a computer system;

(*b*) process or store computer data on behalf of a communication service or users of such service; or

(*c*) own an electronic communications system to provide or offer an electronic communication service;

"sign language" means a language that uses manual communication, body language, facial expressions, lip patterns, hand shapes, orientation and movement of the hands, arms or other parts of the body, other than sound, to communicate or express a person's thoughts;

"spamming" means an illegal attempt or act to deliver a message, over the internet, to someone who has not solicited it;

"stored communication" means communication that has been submitted using a delayed access message service, is stored on equipment, and can be accessed;

"stored recovery information" means information that can be used to decrypt data or electronic

communications;

"sub-domain" means any subdivision of the zm domain name space which begins at the second level domain;

"system interference" means the illegal interception, hindering or data interference of an electronic communications system or computer system, or the inputting, transmission, damage, deletion, deterioration, alteration or suppression of computer data, an electronic communication or its contents through, or by means of, an illegal access;

"TCP/IP" means the Transmission Control Protocol Internet Protocol used by an information system to connect to the internet;

"third party" in relation to a service provider, means a subscriber to the service provider's services, any other user of the service provider's services or a user of information systems;

"TLD" means a top level domain of the domain name system;

"traffic data" means any computer data indicating the electronic communication's origin, destination, route, time, date, size, duration or type of underlying service and any content thereof;

"transaction" means a transaction of either a commercial or non-commercial nature or the provision of information or e-government services, but does not include any banking transaction or electronic funds transferred by a financial institution;

"trespasser" in relation to a computer or electronic communication system, means a person who accesses a computer or electronic communication system without authorisation, but does not include a person authorised by the owner or operator of the computer or electronic communication system to access all or part of the computer or electronic communication system;

"universal access" means access by all citizens of Zambia to internet connectivity and electronic transactions;

"user" means a person or entity who is authorised by a service provider to use its services;

"WAP" means the Wireless Application Protocol; an open international standard developed by the Wireless Application Protocol Forum Limited, a company incorporated under the laws of the United Kingdom, for applications that use wireless communication, and includes internet access from a mobile phone;

"wire communication" means an aural transfer made in whole or in part for the transmission and storage of communications by the aid of wire, cable or other like connection;

"web page" means a data message on the World Wide Web;

"website" means any location on the internet containing a home page or web page;

"World Wide Web" means an information browsing framework that allows a user to locate and access

information stored on a remote computer and to follow references from one computer to related information on another computer;

"Zambia Development Agency" means the Zambia Development Agency established under section 4 of the Zambia Development Agency Act, 2006;

"Zambia Postal Services Corporation" means the Zambia Postal Services Corporation established under the Postal Services Act; and

"zm domain name space" means the .zm ccTLD assigned to the Republic of Zambia according to the two-letter codes in the International Standard ISO.

3. Application

(1) Subject to the other provisions of this section, this Act applies in respect of any electronic transaction or data message.

(2) This Act shall not be construed as—

(*a*) requiring any person to generate, communicate, produce, process, send, receive, record, retain, store or display any information, document or signature by, or in. electronic form; or

(*b*) prohibiting a person from establishing requirements in respect of the manner in which that person will accept data messages.

(3) Sections 5 and 6 of this Act do not apply to the Lands Act.

(4) Part II of this Act does not apply to the Wills and Administration of Testate Estates Act.

(5) This Act shall not be construed as giving validity to any of the following transactions—

(*a*) an agreement for the alienation of immovable property under the Lands Act;