

STATUTORY INSTRUMENTS SUPPLEMENT

to The Uganda Gazette No. 49 Volume CVI dated 30th September, 2013

Printed by UPPC, Entebbe, by Order of the Government.

S T A T U T O R Y I N S T R U M E N T S

2013 No. 42.

THE ELECTRONIC TRANSACTIONS REGULATIONS, 2013

ARRANGEMENT OF REGULATIONS

Regulation

PART I—PRELIMINARY

1. Title
2. Interpretation

PART II—AUTHENTICITY AND INTEGRITY OF DATA MESSAGE

3. Authenticity of data message
4. Self-authenticating data messages
5. Use of harsh marks or metadata
6. Public records
7. Determining the integrity of a data message
8. Specific requirements by public body
9. General information to be provided by a service provider
10. Commercial communications
11. Unsolicited commercial communications
12. Concluding a contract electronically

PART III—TRANSMISSION HOSTING AND CACHING

13. Transmission of data as mere conduit
14. Caching
15. Hosting

Regulation

PART IV—GENERAL

16. Protection of rights
17. Knowledge of service provider
18. Investigation and Monitoring of service providers, sellers and suppliers
19. Procedure for informing authorities about unlawful activities

Offences

20. Failure to provide information

SCHEDULES

Schedule 1- Currency point

Schedule 2- Forms

Form 1- Request of information about alleged illegal activities

Form 2- Direction to give information about alleged illegal activities

Form 3- Information about alleged illegal activities

S T A T U T O R Y I N S T R U M E N T S

2013 No. 42.

The Electronic Transactions Regulations, 2013.

(Under section 35 of the Electronic Transactions Act, 2011, Act No. 8 of 2011)

IN EXERCISE of the powers conferred upon the Minister responsible for information and communications technology by section 35 of the Electronic Transactions Act, 2011, these Regulations are made this 10th day of September, 2013.

PART I—PRELIMINARY

1. Title.

These Regulations may be cited as the Electronic Transactions Regulations, 2013.

2. Interpretation.

In these Regulations unless the context otherwise requires—

“Act” means the Electronic Transactions Act, 2011;

“Authority” means the National Information Technology Authority established by the National Information Technology Authority, Uganda Act, 2009;

“commercial communication” means a communication, in any form, designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial, industrial or craft activity or exercising a regulated profession;

“currency point” has the value assigned to it in Schedule 1;

“service provider” means—

- (a) any public or private entity that provides to the users of its service the ability to communicate by means of a computer system; and

- (b) any other entity that processes or stores computer data on behalf of such a communication service or users of such a service.

PART II—AUTHENTICITY AND INTEGRITY OF DATA MESSAGE

3. Authenticity of data message

(1) For the purposes of section 7 of the Act, where the authenticity of a data message is in issue, the authenticity shall be proved by evidence showing that—

- (a) the data message is self-authenticating;
- (b) the data message has a harsh mark or metadata;
- (c) the data message is a public record; or
- (d) there is factual specificity about the process by which the information is created, acquired, maintained and preserved, including evidence prescribed in sub regulation (2).

(2) The evidence referred to in sub regulation (1) is as follows—

- (a) that the person uses the computer from which the message originates;
- (b) that the computer is reliable;
- (c) that the person has developed a procedure for inserting data into the computer;
- (d) that the procedure has built-in safeguards to ensure accuracy and identify errors such as the computer policy and system control procedures, including—
 - (i) control of access to the database;
 - (ii) control of access to the program;
 - (iii) recording and logging of changes;

- (iv) backup practices; and
- (v) audit procedures to assure the continuing integrity of the records;
- (e) that the person keeps the computer in a good state of repair; and
- (f) that the computer was in working order at the time the witness obtained the readout.

4. Self-authenticating data messages.

For the purposes of regulation (3) (a) a data message is self-authenticating if—

- (a) the message has a sign, inscription, logo, tag or other unique feature identifying it with a particular business, institution or person and the origin of the message is not in dispute;
- (b) the message can be attributed to the originator under section 19 of the Act.

5. Use of harsh marks or metadata

(1) A data message may be authenticated by use of its harsh marks or metadata.

- (2) For the purpose of this regulation—
 - (a) “harsh mark” refers to a unique identifier attached to a data message;
 - (b) “metadata” means information describing the history, tracking, or management of a data message and includes information showing the date or person creating or accessing the data message or transmittal information.

6. Public records

(1) Where a person adduces evidence to show that the office from which the data message was taken is the legal custodian of the message, subject to section 8 of the Act and sub regulation (2), that person shall not be required to prove the accuracy of the message.

(2) The accuracy of the data message referred to in sub regulation (1) shall be relevant in determining the weight to be attached to that data message.

7. Determining the integrity of a data message

The integrity of a data message under section 7(2) of the Act shall be established by assessing the following in respect to the data message—

- (a) the mode of preparing the data message;
- (b) programming errors;
- (c) completeness of the data entry;
- (d) mistakes in output instructions;
- (e) damage and contamination of storage media;
- (f) power outages, and equipment malfunctions;
- (g) improper search and retrieval techniques, data conversion, or mishandling during discovery;
- (h) that the computer used is the standard acceptable type used by the person in issue;
- (i) that the record is given in reliance upon the accuracy of the computer in retaining and retrieving information.

8. Specific requirements by public body

(1) A public body shall before giving notice of the specific requirements applicable to an electronic communication under section 23 of the Act, seek the approval of the Minister.

(2) The Minister shall before giving approval under this regulation confirm that—

- (a) the requirements are consistent with the Act;
- (b) where the requirements involve attaching a signature to the data message, the signature is required to be attached in accordance with the Electronic Signatures Act, 2011;
- (c) the requirements do not stifle the delivery of services to the public and promote the use of electronic communications.

9. General information to be provided by a service provider

(1) A person providing an information system service shall make available to the recipient of the service and any relevant enforcement authority, in a form and manner which is easily, directly and permanently accessible, the following information—

- (a) the name of the service provider;
- (b) the physical address at which the service provider is established;
- (c) the details of the service provider, including his electronic mail address, which make it possible to contact the service provider rapidly and communicate with him or her in a direct and effective manner;
- (d) where the service provider is registered in a trade or similar register available to the public, details of the register in which the service provider is entered and his or her registration number, or equivalent means of identification in that register;
- (e) where the provision of the service is subject to an authorisation scheme, the particulars of the relevant supervisory authority;
- (f) where the service provider exercises a regulated profession—
 - (i) the details of any professional body or similar institution with which the service provider is registered;
 - (ii) the professional title of the service provider;
 - (iii) a reference to the professional rules applicable to the service provider and the means to access them.

(2) Where a service provider refers to prices, these shall be indicated clearly and unambiguously and, in particular, shall indicate whether they are inclusive of tax.

10. Commercial communications

A service provider shall ascertain that any commercial communication provided by the service provider—

- (a) is clearly identifiable as a commercial communication;
- (b) clearly identifies the person on whose behalf the commercial communication is made;
- (c) clearly identifies as such any promotional offer, including any discount, premium or gift; and
- (d) specifies any conditions which must be met to qualify for any offer and the conditions should be easily accessible, and presented clearly and unambiguously.

11. Unsolicited commercial communications

(1) A service provider shall ascertain that any unsolicited commercial communication sent by that service provider electronically, is clearly and unambiguously identifiable as unsolicited, as soon as it is received.

(2) A service provider who contravenes this regulation commits an offence and is liable on conviction to a fine not exceeding six currency points.

12. Concluding a contract electronically

(1) Where a contract is concluded electronically a service provider shall, before an order is placed by the recipient of a service, provide to that recipient in a clear, comprehensible and unambiguous manner the following—

- (a) the different technical steps to follow to conclude the contract;
- (b) whether the concluded contract will be filed by the service provider and whether it will be accessible;

- (c) the technical means for identifying and correcting input errors prior to the placing of the order; and
- (d) the languages offered for the conclusion of the contract.

(2) A service provider shall indicate the relevant code of conduct that the service provider subscribes to and give information on how that code can be accessed electronically.

(3) Where the service provider provides to the recipient, the terms and conditions applicable to the contract, the service provider shall make the terms and conditions available in a way that allows the recipient to store and reproduce them.

(4) Sub regulations (1) and (2) do not apply to contracts concluded exclusively by exchange of electronic mail or by equivalent individual communication.

PART III—TRANSMISSION HOSTING AND CACHING

13. Transmission of data as mere conduit

(1) Where a service is provided which consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, the service provider shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that transmission where the service provider—

- (a) did not initiate the transmission;
- (b) did not select the receiver of the transmission; and
- (c) did not select or modify the information contained in the transmission.

(2) For the purposes of this regulation, transmission or provision of access includes the automatic, intermediate and transient storage of the information transmitted where—

- (a) the storage takes place for the sole purpose of carrying out the transmission in the communication network, and
- (b) the information is not stored for any period longer than is reasonably necessary for the transmission.

14. Caching

Where the electronic service provided consists of the transmission in a communication network of information provided by a recipient of the service, the service provider is not be liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that transmission where—

- (a) the information is the subject of automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request; and
- (b) the service provider—
 - (i) does not modify the information;
 - (ii) complies with conditions on access to the information;
 - (iii) complies with any rules regarding the updating of the information, specified in a manner widely recognised and used by industry;
 - (iv) does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and
 - (v) acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered the removal or disablement.

15. Hosting

Where a service provider offers a service which consists of the storage of information the service provider is not liable for damages or for any other pecuniary remedy or for any criminal sanction as a result of that storage where—

- (a) the service provider—
 - (i) does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or
 - (ii) upon obtaining that knowledge or awareness, acts expeditiously to remove or to disable access to the information; and
- (b) the recipient of the service was not acting under the authority or the control of the service provider.

16. Knowledge of service provider

In determining whether a service provider has actual knowledge for the purposes of regulation 15(a)(i), a court shall consider—

- (a) whether a service provider received notice through any of the means specified in regulation 9; and
- (b) the extent to which any notice includes—
 - (i) the full name and address of the sender of the notice;
 - (ii) details of the location of the information in question; and
 - (iii) details of the unlawful nature of the activity or information in question.

PART IV—GENERAL

17. Protection of rights

- (1) These Regulations shall not be construed —

- (a) to prevent a person from agreeing to different terms in a contract; or
- (b) to affect the right of any party to apply to a court for relief to prevent or stop infringement of any right.

(2) Any power of an administrative authority to prevent or stop infringement of any right shall continue to apply notwithstanding anything to the contrary in these Regulations.

18. Monitoring of service providers, sellers and suppliers

(1) A person may report to the authority any service provider who does not provide the information required under Part IV of the Act.

(2) The authority shall inquire into the report and take necessary action.

19. Procedure for informing authorities about unlawful activities

(1) A competent public authority which requires information from a service provider regarding an alleged illegal activity in accordance with section 32(2) of the Act, shall request for the information from the service provider through the authority.

(2) The request under sub regulation (1) shall be in Form 1 in Schedule 2 to these Regulations.

(3) Upon receipt of the request under sub regulation (1), the authority shall using Form 2 in Schedule 2 direct the service provider to provide the information requested for.

(4) A service provider who provides information to a competent public authority about alleged illegal activities shall specify the information in Form 3 in Schedule 2.

Offences

20. Failure to provide information

A supplier or seller who fails to supply the information required by section 24 of the Act commits an offence and is liable on conviction to a fine not exceeding six currency points.

SCHEDULES

SCHEDULE 1

Regulation 2

Currency point

One currency point is equivalent to twenty thousand shillings.

SCHEDULE 2

Forms

Form 1

Regulation 19(2)

THE REPUBLIC OF UGANDA

THE ELECTRONIC TRANSACTIONS ACT, 2011

THE ELECTRONIC TRANSACTIONS REGULATIONS, 2013.

REQUEST FOR INFORMATION ABOUT ALLEGED ILLEGAL ACTIVITIES

To: THE NATIONAL INFORMATION TECHNOLOGY AUTHORITY
.....
.....

In accordance with section 32 of the Electronic Transactions Act, 2011 this is to request you to provide the following information in respect of
.....

- 1. Name of person
- 2. Address or other Particulars.....

Information required:

.....
.....
.....

Nature and details of alleged illegal activities in respect of which information is required

.....
.....
.....

Dated this day of..... 20....

- 1. Title of person requesting for information:
- 2. Signature.....

THE ELECTRONIC TRANSACTIONS ACT, 2011

THE ELECTRONIC TRANSACTIONS REGULATIONS, 2013.

**DIRECTION TO GIVE INFORMATION ABOUT ALLEGED
ILLEGAL ACTIVITIES**

To (service provider)
.....
.....

In accordance with section 32 of the Electronic Transactions Act, 2011 this is to direct you to provide the following information in respect of the services you provide to:

- 1. Name of person
- 2. Address or other particulars.....

Information required:

.....
.....
.....
.....

**Nature and details of alleged illegal activities in respect of which
information is required**

.....
.....
.....
.....

Dated thisday of..... 20.....

Signature

The National Information
Technology Authority - Uganda

KAMPALA

THE REPUBLIC OF UGANDA

THE ELECTRONIC TRANSACTIONS ACT, 2011
THE ELECTRONIC TRANSACTIONS REGULATIONS 2013

INFORMATION ABOUT ALLEGED ILLEGAL ACTIVITIES

To

Pursuant to section 32 of the Electronic Transactions Act, 2011, this is to bring to your attention the following activities in respect of

- 1. Name of person
- 2. Address or other particulars

Specific nature of activities requested for or to be brought to your attention

.....

Name of service provider

Physical address

Signature

Date

JOHN M. NASASIRA,
Minister of Information and Communications Technology.

