THE REPUBLIC OF UGANDA

THE NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA (NATIONAL DATA BANK) REGULATIONS, 2019

Statutory Instrument No. 109

STATUTORY INSTRUMENTS
SUPPLEMENT No. 36 20th December, 2019

STATUTORY INSTRUMENTS SUPPLEMENT

to The Uganda Gazette No. 64, Volume CXII, dated 20th December, 2019

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

STATUTORY INSTRUMENTS

2019 No. 109.

THE NATIONAL INFORMATION TECHNOLOGY AUTHORITY, UGANDA (NATIONAL DATA BANK) REGULATIONS, 2019

ARRANGEMENT OF REGULATIONS

STATUTORY INSTRUMENTS

2019 No. 109.

The National Information Technology Authority, Uganda (National Data Bank) Regulations, 2019

(Under sections 5(e), 6(e) and 39 of the National Information Technology Authority Uganda Act, 2009)

IN EXERCISE of the powers conferred upon the Minister responsible for information technology by sections 5(e), 6(e) and 39 of the National Information Technology Authority, Uganda Act, 2009, and in consultation with the Board of the National Information Technology Authority, Uganda, these Regulations are made this 13th day of September, 2019.

PART I—PRELIMINARY

1. Title.

These Regulations may be cited as the National Information Technology Authority, Uganda (National Databank) Regulations, 2019.

2. Interpretation.

In these Regulations, unless the context otherwise requires—

"Act" means the National Information Technology Authority, Uganda Act, 2009;

"Authority" means the National Information Technology Authority, Uganda, established by the Act;

"currency point" has the value assigned to it in the Act;

"data" means information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose;

"database" means records of data and the facilities used for the storage of data;

"data controller" means a public body which collects, processes or stores data;

"information" includes data, text, images, sounds, codes, computer programmes, software and databases;

"information and communication technologies" means technologies employed in collecting, filing, storing, using or sending information and includes those technologies involving the use of computers or any telecommunication network;

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

"integration" as used in respect to integration of databases, means the linkage of various databases established by different data controllers into an accessible interface to facilitate real time access and retrieval of information by authorised persons;

"national databank" means the information technology system implemented and managed by the Authority resulting from the integration of various databases established by different data controllers to facilitate real time access and retrieval of information by authorised persons;

"processing" means any operation which is performed upon collected data by automated means or otherwise including—

(a) organisation, adaptation or alteration of the information or data;

(b) retrieval, consultation or use of the information or data;

(c) disclosure of the information or data by transmission; dissemination or otherwise making available; or

(d) alignment, combination, blocking, erasure or destruction of the information or data;

"public body" includes the Government, a department, service or undertaking of the Government, Cabinet, Parliament, a court, local Government administration or a local council and any committee or commission thereof, an urban authority, a municipal council and any committee of such a council, any corporation committee, board, commission or similar body whether corporate or incorporate established by an Act of Parliament relating to undertakings of public services or such purpose for the benefit of the public or any section of the public to administer funds or property belonging to or granted by Government or money raised by public subscription, rates, taxes, cess or charges in pursuance of any written law and any Council, board, committee or society established by an Act of Parliament for benefit, regulation and control of any profession;

"record" includes information that is recorded in any form or in any medium of writing, print, photographic, electronic or otherwise, but does not include a computer programme or other mechanism that can produce a record.

PART II—CREATION AND MANAGEMENT OF THE NATIONAL DATABANK

3. Creation and management of national databank

(1) There is created a national databank which shall consist of databases established and maintained by data controllers.

(2) The Authority shall manage the national databank.

(3) For the purposes of this regulation, every data controller shall link its database to the national databank as prescribed by the Authority.

(4) The Authority shall—

(a) take appropriate security measures for the prevention of unauthorised access, alteration, disclosure, accidental loss, and destruction of the data in the national databank;

(b) receive, document and ensure that all complaints in relation to the national databank are resolved;

(c) co-operate with other countries to the extent necessary for exchanging relevant information in accordance with the law;

(d) issue codes of practice or guidelines to data controllers whose databases are linked to the national databank to employ adequate and effective security controls to protect the confidentiality, integrity and availability of the national databank;

(e) take all reasonable steps to ensure that any person employed in the Authority is aware of and complies with the security measures regarding the security of the national databank; and

(f) do anything incidental or conducive to give effect to these Regulations.

4. Data controllers to safeguard database linked to national databank

Every data controller shall be responsible for the integrity and confidentiality of data in its database and shall for that purpose take appropriate, reasonable, technical, security and organisational measures to prevent—

(a) loss, damage or unauthorised destruction of data; and

(b) unlawful access or processing of data or other information in its database.

5. Accessing information in national databank.

(1) The Authority may grant access to the national databank to—

(a) authorised staff of the Authority;

(b) data controllers;

(c) a public body; and

(d) any person on such conditions as may be specified by the Authority.

(2) The access to the national data bank shall be in accordance with user rights and access levels prescribed by the Authority.

(3) For the avoidance of doubt, where a fee is chargeable for access to data, a person shall be required to make a payment before the access to the national databank is granted.

6. Authority to create access levels.

(1) The Authority shall for the purposes of safeguarding a database that is linked to the national data bank, create levels of accessing the database in the national databank.

(2) A person shall not use the national databank to unlawfully access a database.

(3) A person who contravenes subregulation (2) commits an offence and is liable on conviction—

(a) to a fine not exceeding forty-eight currency points or imprisonment not exceeding twenty-four months or both;

(b) in the case of a second or subsequent offence, a fine not exceeding seventy-two currency points or imprisonment not exceeding three years or both;

(c) in the case of a continuing offence, an additional fine not exceeding ten currency points for each day on which the offence continues.

(4) A court which convicts a person under this regulation may order the forfeiture to the State of anything used in connection with the commission of the offence.

7. Updating of database.

Every data controller shall be responsible for updating its database and ensure that the database is complete and accurate.

PART IV—REGISTRATION OF DATABASE

8. Database registration and index of databases.

(1) The Authority shall keep and maintain a register of databases in the national databank.

(2) The Authority shall register in the register of databases, the name of the database, the data controller and the purpose for which the data is collected and processed.

PART V—SECURITY OF INFORMATION

9. Notification of data security breach.

(1) Where a person unlawfully accesses or compromises a database linked to the national databank, the data controller responsible for such a database shall notify the Authority and immediately take appropriate measures to remedy the breach.

(2) Without prejudice to subregulation (1), the notification shall not be made later than twenty-four hours after the discovery of the breach.

(3) The notification under subregulation (1) shall include the measures taken by the data controller in respect of—

(a) reporting the breach to the relevant law enforcement body;

(b) determining the scope of the breach and the preliminary remedial action to counter the breach; and

(c) restoration of the integrity of the database.

§(4) Where the Authority receives a notification under subregulation (1) (a), the Authority shall within twenty-four hours, take appropriate action to safe guard the national databank.

(5) Where a person unlawfully accesses or compromises the national databank, the Authority shall notify the various data controllers whose databases are linked to the national databank and immediately take appropriate measures to remedy the breach.

(6) The notification under subregulation (5) shall include the measures taken by the Authority in respect of—

(a) reporting the breach to the relevant law enforcement body;

(b) determining the scope of the breach and the preliminary remedial action to counter the breach; and

(c) restoration of the integrity of the national databank.

(7) Where a data controller is notified of a breach under subregulation (5), the data controller shall within twenty-four hours take appropriate action to safeguard the database.

PART VI—MISCELLANEOUS

10. Complaints regarding national databank.

(1) The Authority shall receive and record every complaint made in respect of the national databank.

(2) The Authority may, after considering a complaint, direct a data controller to remedy any breach or take such action as the Authority considers appropriate to resolve the complaint.

11. Power to carry out security checks.

(1) The Authority may, at any reasonable time, carry out inspection and assessment of the security measures put in place by a data controller.

(2) Where the inspection carried out under subregulation (1) reveals any breach of these Regulations, the Authority shall direct the data controller to remedy any breach or take such action as the Authority may specify.

12. Research into developments in database maintenance.

For the purposes of these Regulations, the Authority shall undertake research into, and monitor developments in data processing, including data linkage and information and communication technologies and ensure that there are no significant risks of any adverse effects to the national databank.

13. Authority to monitor compliance.

(1) The Authority shall carry out periodical audits of the databases of data controllers to ensure compliance with these Regulations.

(2) For the purposes of subregulation (1), a data controller shall grant access to its database to the Authority.

(3) The Authority shall monitor compliance of the data controllers with the requirements of these Regulations, prepare and submit quarterly reports to the Minister and the office of the Prime Minister.

(4) The Minister shall submit the reports under subregulation (1) to the Cabinet.

FRANK TUMWEBAZE (MP.)
Minister of Information and Communications Technology and National Guidance