THE REPUBLIC OF UGANDA

THE DATA PROTECTION AND PRIVACY REGULATIONS, 2021.

Statutory Instrument No. 21 of 2021

STATUTORY INSTRUMENTS
SUPPLEMENT No. 10 12th March, 2021

STATUTORY INSTRUMENTS SUPPLEMENT

to The Uganda Gazette No. 23, Volume CXIV, dated 12th March, 2021

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

STATUTORY INSTRUMENTS

2021 No .21.

THE DATA PROTECTION AND PRIVACY REGULATIONS, 2021

Regulation

PART IV—DATA PROTECTION REGISTER

PART V—REGISTRATION OF DATA COLLECTORS, DATA PROCESSORS AND DATA CONTROLLERS

Procedure for considering application

Grant or refusal of registration

PART VI—DATA CORRECTION AND PROCESSING

SCHEDULES

SCHEDULE 1—FORMS

Form 1 — Notice of Objection to Collection/Processing of Personal Data

Form 2 — Application for Registration/Renewal of Registration

Form 3 — Undertaking Not to Process or Store Personal Data Outside Uganda

Form 4 — Certificate of Registration

Form 5 — Application for Certified Copy of Extract/Entry in Register

Form 6 — Complaint Concerning Processing Personal Data Without Appropriate Security Measures

Form 7 — Notification of Data Breach

Form 8 — Request to Confirm Possession of Personal Data

Form 9 — Complaint Concerning Inaccurate Personal Data in the Possession of Data Controller

Form 10 — Decision On Complaint in Respect of Inaccurate Personal Data in the Possession of Data Controller

Form 11 — Complaint Concerning Infringement or Violation of the Act

Form 12 — Decision of the Office on Compliant Concerning Infringement or Violation of the Act

Form 13 — Appeal

Form 14 — Decision of Minister on Appeal

SCHEDULE 2 — Fees

2021 No. 21.

The Data Protection and Privacy Regulations, 2021

(Under section 39 of the Data Protection and Privacy Act, 2019, Act 9 of 2019)

IN EXERCISE of the powers conferred upon the Minister by section 39 of the Data Protection and Privacy Act, 2019, and after consultation with the National Information Technology Authority - Uganda, these Regulations are made this 29th day of January, 2021.

PART I—PRELIMINARY

1. Title

These Regulations may be cited as the Data Protection and Privacy Regulations, 2021.

2. Interpretation

In these Regulations, unless the context otherwise requires—

"Act" means the Data Protection and Privacy Act, 2019;

"applicant" means a data collector, data processor or data controller who makes an application for registration under these Regulations;

"Board" means the Board of Directors appointed under the National Information Technology Authority, Uganda, Act, 2009;

"Director" means the National Personal Data Protection Director appointed under section 4(2) of the Act;

"Minister" means the Minister responsible for information and communications technology;

"Office" means the Personal Data Protection Office established by section 4(1) of the Act;

"Register" means the Data Protection Register kept and maintained by the Office under section 29 of the Act.

PART II—PERSONAL DATA PROTECTION OFFICE

3. Establishment of Personal Data Protection Office

(1) There is established a Personal Data Protection Office in the National Information Technology Authority, Uganda which shall be responsible for personal data protection and privacy.

(2) The Office shall be under the general supervision of the Board.

(3) For the purposes of section 5(3) of the Act—

(a) the Board shall ensure that the Office, in the performance of its functions, is independent and not subject to the direction or control of any person or authority; and

(b) the affairs of the National Information Technology Authority, Uganda are managed separately from the affairs of the Office.

4. Additional functions of Personal Data Protection Office

In addition to the functions specified in section 5 of the Act, the Office shall—

(a) provide guidance to data collectors, data processors, data controllers, and data subjects about their data protection and privacy rights, obligations and responsibilities under the Act;

(b) coordinate, supervise and monitor data collectors, data processors, data controllers and data subjects on all matters relating to the Act;

(c) build capacity of management of the Office and staff on compliance requirements under the Act and these regulations;

(d) set, monitor and regulate standards for personal data protection and privacy;

(e) conduct audits to ensure compliance by data collectors, data processors, data controllers and data subjects with the Act and these regulations and address potential issues pro-actively;

(f) provide guidance to Government on matters of data protection and privacy;

(g) undertake or commission research as may be necessary to promote the objects of the Act; and

(h) issue recommendations to institutions about the interpretation or application of data protection and privacy rules.

5. Powers of Office

In carrying out the functions specified under the Act, the Office may—

(a) establish a mechanism for collaboration and promotion of partnerships between various categories of players in the data protection and privacy aspects; and

(b) charge fees for services provided by the Office.

6. Office to cooperate with other authorities

(1) The Office shall cooperate with other government ministries, departments and agencies in the implementation of the Act and regulations.

(2) For the purpose of subregulation (1), all ministries, departments and agencies of government shall accord to the Office such assistance as may be necessary to ensure proper discharge of the functions.

7. National Personal Data Protection Director

(1) The Office shall be headed by a National Personal Data Protection Director appointed on such terms and conditions as may be specified in his or her instrument of appointment.

(2) The Director shall be appointed by the Minister on the recommendation of the Board.

(3) Without limiting the general effect of subregulation (1), the Director shall hold office for five years and is eligible for re-appointment for one more term.

(4) The Director shall be a person of high moral character, proven integrity and with qualifications in law and experience in data protection and privacy matters or any other related field.

(5) The Minister may, after consultation with the Board, terminate the appointment of the Director for—

(a) abuse of office;

(b) corruption;

(c) incompetence;

(d) physical or mental incapacity that renders the Director incapable of performing the duties of the Office;

(e) conviction for an offence involving moral turpitude;

(f) being adjudged bankrupt by a court of law; or

(g) any other reasonable ground.

8. Functions of National Personal Data Protection Director

Subject to the general supervision and direction of the Board, the Director shall be responsible for—

(a) the management and operations of the Office;

(b) the management of the funds, property and business of the Office;

(c) the administration, organisation and control of officers and staff of the Office;

(d) any other duties as the Board may specify.

9. Other officers and staff of Office

(1) The Office shall consist of such other officers and staff as may be necessary for the proper functioning of the Office, appointed on such terms and conditions as may be specified in their instruments of appointment.

(2) For the purposes of subregulation (1), the Board may, on the advice of the Director, appoint other officers and staff of the Office.

(3) The Board shall be responsible for the promotion, training and discipline of officers and staff of the Office.

PART III—DATA COLLECTION AND PROCESSING

10. Objection to collection and processing of data

(1) Subject to subregulation (2), a data subject who objects to the collection or processing of his or her personal data, shall notify the data collector, data processor or data controller of the objection.

(2) Subregulation (1) does not apply—

(a) to personal data collected or processed under section 7(2) of the Act; and

(b to personal data which is subject to the legitimate interest of a data collector, data processor or data controller.

(3) For the purposes of subregulation (2)(b), "legitimate interest" is the processing of personal data in a manner that the data subject would reasonably expect or where there is a compelling justification for the processing and includes the processing of data to

prevent fraud, maintain network and information security, prevention of crime or threats to public security, internal administrative purposes.

(4) The burden to establish a legitimate interest lies with the data collector, data processor or data controller.

(5) The notification referred to in subregulation (1) shall be in Form 1 in Schedule 1.

11. Personal data relating to children

For the purposes of section 8 of the Act, every data collector, data processor and data controller shall establish a system to ascertain the age of persons whose personal data is to be collected, processed or stored, and where the data relates to a child, the manner of obtaining consent of a parent or legal guardian, where necessary.

12. Data protection impact assessment

(1) Where the collection or processing of personal data poses a high risk to the rights and freedoms of natural persons, the data collector, data processor or data controller shall, prior to the collection or processing, carry out an assessment of the impact of the envisaged collection or processing operations on the protection of personal data.

(2) Every data protection impact assessment shall include—

(a) a systematic description of the envisaged processing and the purposes of the processing;

(b) an assessment of the risks to personal data and the measures to address the risks; and

(c) any other matter the Office may require.

(3) The Office shall establish and make public a list of the processing operations which are subject to the requirement for a data protection impact assessment under subregulation (1).

13. Data Protection Register

(1) The Data Protection and Privacy Register kept and maintained by the Office under section 29 of the Act shall be in electronic or manual form.

(2) The Office shall keep the Register up to date.

14. Information contained in Register

(1) The Register shall contain information relating to data collectors, data processors and data controllers including the purpose for which personal data is collected or processed.

(2) Without limiting the general effect of subregulation (1), the Register shall in respect to every person, institution or public body required to be registered contain the following—

(a) the name of the person, institution or public body;

(b) the address of the person, institution or public body;

(c) the nature of the personal data being collected or processed by the person, institution or public body; and

(d) the purpose for the collection or processing of personal data.

PART V—REGISTRATION OF DATA COLLECTORS, DATA PROCESSORS AND DATA CONTROLLERS

15. Data collectors, data processors and data controllers to register with Office

(1) Subject to subregulation (2), every data collector, data processor or data controller shall register with the Office.

(2) The Office shall, in consultation with the Board, by notice in the Gazette, exempt certain data collectors, data processors or data controllers from the requirement to register with the Office.

(3) A person who contravenes subregulation (1) commits an offence and is liable, on conviction, to a fine not exceeding six currency points or imprisonment not exceeding three months or both.

(4) Where the offence in subregulation (3) is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully authorises the contravention commits an offence and is liable, on conviction, to the penalty and fine specified in subregulation (3).

16. Application for registration

(1) An application for registration shall be in Form 2 in Schedule 1 and shall be accompanied by the fee specified in Schedule 2.

(2) Notwithstanding the general effect of subregulation (1), an application shall—

(a) state the name of the applicant,

(b) state the name and address of the applicant's representative, where the applicant is a foreigner or situated outside Uganda;

(c) specify whether the applicant is a data collector, data processor or data controller;

(d) state the address of the applicant;

(e) specify the nature and category of personal data being processed or is to be processed;

(f) specify the purpose for which the applicant collects or processes personal data;

(g) contain a description of the purpose for which the personal data is being processed or collected;

(h) specify the duration for which personal data shall be kept;

(i) contain a description of the recipient to whom the applicant intends to disclose the personal data, if any;

(j) specify the details of the data protection officer, if any;

(k) specify the name of the country to which the applicant may transfer the data, if any;

(l) contain a general description of measures to be taken to secure the personal data; and

(m) contain any other information that the Office may require.

(3) Every application shall be accompanied by a written undertaking by the applicant not to process or store personal data in a country outside Uganda unless such country has adequate measures in place, at least equivalent to the protection provided for by the Act for the protection of the personal data and the data subject consents to the transfer.

(4) The written undertaking referred to in subregulation (3) shall be in Form 3 in Schedule 1.

(5) An applicant who knowingly gives false information in support of an application for registration commits an offence and is liable, on conviction, to a fine not exceeding six currency points or imprisonment not exceeding three months or both.

(6) Where the offence in subregulation (5) is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully gives false information commits an offence and is liable, on conviction, to the penalty and fine specified in subregulation (5).

Procedure for considering application

17. Procedure for considering application

(1) Upon receipt of an application, the Office shall review the application to ensure that all the relevant documents and information are available to enable the processing of the application.

(2) Where, upon review of an application under subregulation (1), the Office finds that the application is incomplete, the Office shall request the applicant to provide additional information or clarify the information provided.

(3) The Office may carry out any investigation or audit in respect to any application to enable the making of a decision.

18. Report in respect of application

(1) The Office shall, within thirty days after receipt of an application or additional information, investigate and prepare a detailed report in respect of an application to enable the processing of the application.

(2) The Office shall, in considering an application under this regulation, have regard to the the nature and category of personal data to be collected or processed by the applicant.

(3) The decision to register or not to register the applicant shall be made within fifteen days after the report is made.

Grant or refusal of registration

19. Grant of registration and issue of certificate

(1) After considering an application, the report under regulation 18 and the Office is satisfied that the applicant meets the requirements for registration, the Office shall grant the application and issue a certificate of registration.

(2) A certificate of registration shall be in Form 4 in the Schedule 1.

20. Validity of registration

A registration shall be valid for twelve months from the date of registration.

21. Refusal of registration

(1) After considering an application, the report under regulation 18 and the Office is satisfied—

(a) that the applicant does not meet the requirements for registration;

(b) that the particulars provided for inclusion in the Register are insufficient; or

(c) the appropriate safeguards for the protection of the privacy of data subjects have not been provided by the applicant,

the Office shall not grant the application for registration.

(2) The decision in subregulation (1) shall be communicated in writing and shall include the reasons for the refusal.

(3) The refusal of an application for registration is not a bar to the applicant making a fresh application.

22. Review of decision

(1) A person dissatisfied with the decision of the Office may appeal to the Minister.

(2) The appeal under subregulation (1) shall be handled in accordance with the appeals procedure specified in regulation 46.

23. Renewal of registration

(1) A holder of a certificate of registration may apply for renewal of the registration.

(2) An application for renewal shall be made at least three months before the expiry of the current registration.

(3) An application for renewal shall be in Form 1 in Schedule 1 and shall be accompanied by the fee set out in Schedule 2.

24. Cancellation of registration

(1) Subject to subregulation (2), the Office may cancel registration for any good cause.

(2) Registration shall not be canceled unless the person to whom the proposed cancellation relates, is afforded a reasonable opportunity to be heard.

25. Removal from Register

(1) Where—

(a) a person registered under these regulations ceases to collect or process personal data; or

(b) the registration of a person is cancelled,

the Office shall remove the details of such person from the Register.

(2) A person registered under these regulations who ceases to collect or process personal data shall, in writing, notify the Office within thirty days of ceasing to collect or process personal data.

26. Effect of ceasing to collect and process data

(1) Section 3(1)(d) of the Act shall apply to a data collector, data processor or data controller who ceases to collect or process personal data.

(2) Without limiting the general effect of subregulation (1), a data collector, data processor or data controller who ceases to collect or process personal data shall ensure that any personal data in the possession of the data collector, data processor or data controller is secure and treated in accordance with the Act.

27. Duty to notify changes of information in Register

A data collector, data processor or data controller in respect of whom an entry is made in the Register shall notify the Office in writing of any change in the registered particulars of the data collector, data processor or data controller within fourteen days of the occurrence of the change.

28. Search and inspection of Register

(1) The Register shall at all reasonable times be available for search or inspection by any person free of charge.

(2) Any person may, on payment of the fee set out in Schedule 2, obtain a certified copy of an extract or entry in the Register.

(3) An application to obtain a certified copy of an extract or entry in the Register shall be in Form 5 in Schedule 1.

PART V—DATA CORRECTION AND PROCESSING

29. Request to correct or delete personal data

(1) A data subject may, in writing, request a data controller –

(a) to correct or delete personal data about the data subject held by or under the control of the data controller that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

(b) to destroy or delete a record of personal data about the data subject held by the data controller which the data controller no longer has the authority to retain.

(2) On receipt of the request under subregulation (1), the data controller shall consider the request and inform the data subject in writing of its decision within seven days after receipt of the request.

(3) Where the data controller is satisfied with the request under subregulation (1), the data controller shall in accordance with section 16(2) of the Act, comply with the request.

(4) Where the data controller cannot comply with the request, the data controller shall, in writing, inform the data subject of the rejection, the reasons for the rejection, and any action taken as a result of the request.

(5) Where the data controller complies with the request under subregulation (3), the data controller shall inform each person to whom the personal data has been disclosed of the correction made and the action taken as a result of the request.

(6) The manner of informing persons of the correction made under subregulation (5) shall be determined by the data controller taking into consideration the correction made, the nature of the personal data and the number of persons to whom the change made has to be communicated.

30. Processing personal data outside Uganda

(1) A data collector, data processor or data controller shall not process or store personal data outside Uganda unless such data collector, data processor or data controller demonstrates to the Office—

(a) that the country outside Uganda where the personal data is to be processed or stored has adequate measures in place for the protection of the personal data at least equivalent to the protection provided for by the Act; or

(b) that the data subject has consented to the processing or storing of personal data outside Uganda.

(2) Any personal data processed outside Uganda in accordance with subregulation (1), shall not be further transferred to, or processed in, a third country without the express consent of the data subject.

(3) The consent of a data subject required under section 19 and subregulation (1) shall be obtained in manner and form that takes into consideration the nature of the personal data sought to be processed or stored outside Uganda.

(4) The Office shall, for the purposes of subregulation (1)(a), specify, by notice in the Gazette, the countries which have adequate measures in place for the protection of the personal data at least equivalent to the protection required by the Act.

(5) Where a data collector, data processor or data controller wishes to process or store personal data in a country that does not appear on the list of countries referred to in subregulation (3), it is the responsibility of the data collector, data processor or data controller to prove that that country has adequate measures in place for the protection of the personal data at least equivalent to the protection provided for by the Act.

(6) A data collector, data processor or data controller who, without lawful or reasonable excuse, fails to comply with this regulation commits an offence and is liable, on conviction, to a fine not exceeding two currency points for each day the person is in default or imprisonment not exceeding three months or both.

PART VI—SECURITY OF DATA

31. Publication of personal data security practices and procedures

(1) For the purposes of section 20(3) of the Act, the Office shall publish, in the *Gazette*, the generally accepted information security practices and procedures and specific industry professional rules and regulations applicable to the security of personal data.

(2) Information security practices and procedures and specific industry professional rules and regulations applicable to the security of personal data referred to in subregulation (1) include—

(a) administrative measures, that is to say, measures aimed at creating efficient guidelines and security standards for dealing with personal data;

(b) technical measures, that is to say, measures aimed at preventing overlap and restricting access to systems and personal data

(3) All data collectors, data processors and data controllers shall comply with the generally accepted information security practices and procedures and specific industry professional rules and regulations published by the Office under this regulation.

32. Security measures by data controller

(1) For the purposes of section 21 of the Act, a data controller shall ensure that any data processor that processes personal data for the data controller develops and implements appropriate security measures to safeguard the personal data.

(2) A data subject or any person who believes that a data processor is processing personal data in contravention of this regulation may make a complaint to the Office.

(3) The complaint shall be in Form 6 in Schedule 1.

(4) The complaint shall be handled in accordance with the complaints procedure specified in the Act and these Regulations.

33. Notification of data security breaches

(1) The notification required under section 23(1) of the Act shall be made immediately after the occurrence of the data breach.

(2) The notification of a data breach shall be in Form 7 in Schedule 1.

(3) Notwithstanding subregulation (2), the notification shall include the following—

(a) the nature of the personal data breach;

(b) the personal data which is the subject of the data breach;

(c) the categories and approximate number of data subjects affected by the personal data breach;

(d) the likely consequences of the personal data breach;

(e) the appropriate remedial measures taken or proposed to address the personal data breach; and

(f) the name and contact details of the data protection officer or other point of contact.

(4) The Office shall, immediately after receiving a notification referred to in subregulation (1), provide the concerned data collector, data processor or data controller with appropriate guidance on how to deal with the data breach.

(5) The guidance referred to in subregulation (4) shall include—

(a) the remedial measures that should be taken by the data collector, data processor or data controller to deal with the data breach;

(b) the manner of notification of the data subject affected by the data breach including requiring the data collector, data processor or data controller to provide the data subject with sufficient information relating to the data breach in order to allow the data subject to take protective measures against the consequences of the data breach;

(c) any measures to alert the general public on the nature of the data breach; and

(d) any additional recommended remedial measures, if any.

PART VII—RIGHTS OF DATA SUBJECTS

34. Processing or collection information without consent

(1) A data collector, data processor or data controller who collects or processes personal data without the prior consent of the data subject in contravention of section 7(1) of the Act, commits an offence and is liable, on conviction to a fine not exceeding three currency points for each day that the contravention continues or to imprisonment not exceeding six months or both.

(2) Where the offence in subregulation (1) is committed by a corporation, the corporation and every officer of the corporation who knowingly and wilfully authorises the collecting or processing of personal data in contravention of section 7(1) of the Act, commits an offence and is liable, on conviction, to a fine specified in subregulation (1)

(3) A court that convicts a data collector, data processor or data controller under subregulation (1) may in addition to the fine or imprisonment direct the Office to revoke the registration of the person.

35. Right to access personal information

(1) The request by a data subject to a data controller to confirm whether the data controller holds personal information on the data subject shall be in Form 8 in Schedule 1.

(2) For the purposes of section 24(1) of the Act, a data subject satisfies the requirement of proof of identity, where the data subject provides any of the following—

(a) a national identification card or aliens identification card;

(b) a passport or any travel document; or

(c) a drivers licence.

(3) A data controller shall inform the data subject of its decision within seven days after receipt of the request.

(4) Where a data controller refuses the request of the data subject, the data controller shall state the reasons for the refusal.

36. Right to prevent processing of personal data

(1) A data subject may, by notice in writing to a data controller or data processor, require the data controller or data processor to cease the processing or further processing of personal data where the processing or further processing is not compatible with the purpose for which the personal data was collected.

(2) A data controller or data processor shall, within fourteen days after receipt of the notice, inform the data subject in writing that the data controller or data processor has complied or intends to comply with the notice of the data subject.

(3) Where a data controller or data processor does not comply with the notice, the data controller or data processor shall state the reasons for non-compliance.

(4) Where the data controller gives reasons for non-compliance, a copy of the notice required by subregulation (2) shall be given to the Office within seven days.

(5) Where the Office does not agree with the reasons for non-compliance, the Office shall direct the data controller or data processor to comply with the notice of the data subject within seven days.

37. Right to appeal decision to continue processing personal data

(1) Where a data processor or data controller notifies the data subject of his or her intention to continue processing personal data for the purpose of direct marketing, the data subject may within fourteen days of receiving the notice request the Office in writing to review the decision of the data controller or data processor.

(2) The Office shall review the decision of the data controller or data processor within fourteen days after receiving the request of the data subject.

38. Rights in relation to automated decision making

(1) A data subject shall refuse by notice in writing to a data controller or data processor, require the data controller or data processor to ensure that any decision taken by or on behalf of the data controller or data processor which significantly affects the data subject is not based solely on the processing by automatic means.

(2) A data processor or data controller shall, within fourteen days after receipt of a notice, inform the data subject in writing that the data controller or data processor has complied or intends to comply with the notice of the data subject.

(3) Where a data processor or data controller does not comply with the notice, the data controller or data processor shall state the reasons for non-compliance.

(4) Where a data processor or data controller gives reasons for non-compliance, a copy of the notice required by subregulation (2) shall be given to the Office within fourteen days after giving reactions for noncompliance.

(5) Where the Office is satisfied that the data subject is justified, the Office shall direct the data processor or data controller to comply with the notice of the data subject within seven days after receiving the directive.

39. Rectification, blocking, erasure and destruction of personal data

(1) Where a data subject believes that a data controller holds inaccurate personal data about the data subject, the data subject may request, in writing, the data controller to rectify, block, erase and destroy that personal data.

(2) Where the data controller does not comply with the request of the data subject under subregulation (1) within thirty days of receipt of the request, the data subject may make a complaint to the Office.

(3) The complaint referred to in subregulation (1) shall be in Form 9 in Schedule 1.

(4) The Office shall consider the complaint of the data subject and inform the data subject and data controller of its decision within seven days after receipt of the complaint.

(5) The decision of the Office shall be in Form 10 in Schedule 1.

(6) Notwithstanding subregulation (3), where the decision of the Office is that personal data of a data subject held by a data controller is inaccurate, the Office may—

(a) order the data controller to rectify, update, block, erase or destroy the personal data; or

(b) direct the data controller to update the statement of the true facts which the Office considers appropriate.

(7) Where the Office makes an order under subregulation (6)(a), the Office shall require the data controller to notify all third parties to whom such personal data had been previously disclosed to and the fact that such data has been rectified, updated, blocked, erased or destroyed.

(8) The Office shall specify the mode of notification and the time within which the data controller may make the notification under subregulation (7).

PART VIII—COMPLAINTS AND INVESTIGATIONS

40. Complaints handling by data collectors, data processors and data controllers

Every data collector, data controller and data processor shall develop and implement a complaints handling system to deal with complaints from data subjects.

41. Complaints against breach and noncompliance

(1) Where—

(a) a data subject or any person believes that a data collector, data processor or data controller is infringing on his or her rights or is in violation of the Act, the data subject or person may make a complaint to the Office; or

(b) the Director is of the opinion that a data collector, data processor or data controller is infringing or is in violation of the Act, the Director may serve a notice on such data collector, data processor or data controller requiring the data collector, data processor or data controller to take such remedial action within such period as may be specified in the notice.

(2) For the purposes of subregulation (1)(a), a complaint shall be in Form 11 in Schedule 1.

(3) Every complaint shall be addressed to the Director.

(4) This regulation does not apply to complaints made under regulation 39(3).

42. Office to investigate complaints

(1) Where a complaint is made to the Office under regulations 39 or 41, the Office shall investigate the complaint within twenty-one days after receipt of the complaint.

(2) The Office may, for the purpose of investigating a complaint, issue a written notice requiring any person—

(a) to attend at a specified time and place for the purpose of being examined orally in relation to the complaint;

(b) to produce any document, record or article as may be required with respect to any matter relevant to the investigation; or

(c) to furnish a statement in writing made under oath or on affirmation setting out all information which may be required under the notice.

(3) A notice issued under subregulation (2) shall be signed by the Director.

(4) A person to whom a notice under subregulation (2) is served shall—

(a) comply with the notice;

(b) appear before the Office in accordance with the terms of the notice; and

(c) answer any questions, produce any documents, records or statement, as may be required with respect to any matter relevant to the investigation.

(5) The Office may require the person producing a document, record or statement to give an explanation relating to the document, record or statement.

(6) Where material to which an investigation relates consists of information stored or recorded in an electronic record system or information system, the notice may require the person named to give access to or produce the information in a form in which it is visible and legible for purposes of the investigation.

(7) A person who, without lawful or reasonable excuse, fails to comply with the notice issued under subregulation (2) or who furnishes to the Office any information which he or she knows to be false or misleading commits an offence and is liable on conviction to a fine not exceeding two currency points for each day the person is in default or imprisonment not exceeding three months or both.

(8) Subject to this regulation, the Office shall regulate the handling of complaints, investigations and conduct of hearings in such manner as it may determine.

(9) The Office shall observe fairness and the principles of natural justice in handling complaints under this regulation.

43. Preservation of information during investigation

(1) Where the Director is of the opinion that information required for an investigation is vulnerable to loss or modification, the Director may apply to a competent court for an order to preserve the information.

(2) An order preserving information may be issued in respect of information stored or recorded in an electronic record system or information system including traffic data.

(3) An order made under subregulation (1) shall remain in force until such time as may reasonably be required for the investigation of the complaint to be finalised.

44. Director may seek assistance in investigation

For the purpose of gathering information or for the proper conduct of any investigation under these regulations, the Director may seek the assistance of any person or authority.

45. Decision on complaint

(1) The Office shall consider and determine a complaint within thirty days after receipt of the complaint.

(2) A decision of the Office on a compliant shall be in Form 12 in Schedule 1.

(3) Notwithstanding subregulation (1), where the Office determines that a data collector, data processor or data controller is infringing on the rights of a data subject or is in violation of the Act, the Office shall serve on such data collector, data processor or data controller a notice requiring the data collector, data processor or data controller—

(a) to take or refrain from taking the steps specified within the time stated in the notice;

(b) to refrain from processing any personal data or personal data of a description specified in the notice;

(c) to refrain from processing personal data except in accordance with directions contained in the notice; or

(d) to take any remedial action specified in the notice.

(4) In deciding whether to serve a notice under subregulation (3), the Office shall consider whether the contravention has caused or is likely to cause damage or distress to any person.

(5) A notice issued in respect of a contravention of a provision of the Act may also require the data collector, data processor or data controller to rectify, block, erase or destroy other data held by the

data collector, data processor or data controller and which contains an expression of opinion which appears to the Office to be based on the inaccurate data.

(6) Where—

(a) a notice requires the data controller to rectify, block, erase or destroy personal data; or

(b) the Office is satisfied that personal data which has been rectified, blocked, erased or destroyed was processed in contravention of the Act,

the Office may require the data collector, data processor or data controller to notify a third party to whom the data has been disclosed of the rectification, blocking, erasure or destruction.

(7) A person dissatisfied with the decision of the Office may appeal to the Minister in accordance with regulation 46.

46. Appeals

(1) A person aggrieved by a decision on a complaint or a decision made by the Office under the Act or these regulations shall appeal to the Minister in Form 13 in Schedule 1.

(2) An appeal to the Minister shall be made within thirty days from the date of the notice of the decision to be appealed against.

(3) An appeal shall be addressed to the Permanent Secretary of the Ministry responsible for information and communications technology for the attention of the Minister.

(4) A copy of the appeal shall be provided to the Office by the person making the appeal.

(5) The Minister shall consider the appeal and communicate his or her decision within thirty days after receipt of the appeal.

(6) For the purposes of subregulation (5), the Minister may constitute a committee comprising senior officials in the Ministry or any other Ministry, Department or agency of Government to assist him or her consider and determine an appeal.

(7) The decision of the Minister shall be in Form 14 in Schedule 1.

PART X—GENERAL

47. Designation of data protection officer

(1) For the purposes of section 6 of the Act and subject to subregulation (2), the Office shall specify the persons, institutions and public bodies required to designate a data protection officer under the Act.

(2) Every person, institution or public body that processes or controls personal data shall designate a data protection officer where—

(a) the activities of the person, institution or public body, consist of processing operations which by virtue of their nature, scope or purpose require regular and systematic monitoring of data subjects on a large scale; or

(b) the core activities of the person, institution or public body consist of processing of special personal data in accordance with the Act.

(3) The responsibilities of a data protection officer are—

(a) to conduct regular assessments and audits to ensure compliance with the Act;

(b) to serve as the point of contact between the person, institution or public body, and the Office;

(c) to maintain records of all data processing activities conducted by person, institution or public body;

(d) to respond to data subjects and to inform them about how their personal data is being used and what measures the person, institution or public body, has put in place to protect the data; and

(e) to ensure that data subjects' requests to see copies of their personal data or to have their person data erased are fulfilled or responded to, as necessary.

(4) Every person, institution or public body that designates a data protection officer shall provide such data protection officer with the relevant training to enable him or her perform the duties of a data protection officer.

(5) For the purposes of determining what constitutes "large scale" under subregulation (2), the following shall be taken into consideration—

(a) the number of data subjects concerned, either as a specific number or as a proportion of the relevant population;

(b) the volume of data or the range of different data items being processed;

(c) the duration, or permanence of the data processing activity; or

(d) the geographical extent of the processing activity.

(6) Subregulation (2) does not apply to courts of law acting in their judicial capacity.

48. Failure to comply with notice

A person who fails to comply with any notice issued by the Office under these regulations commits an offence and is liable, on conviction, to a fine of not exceeding three currency points for each day in default of the notice or to imprisonment not exceeding six months or both.

49. Authority to monitor compliance.

(1) The Office shall monitor compliance of every data collector, data processor, data controller with the Act and the requirements of these Regulations; and shall prepare and submit an annual compliance report to the Minister and the Office of the Prime Minister.

(2) The Minister shall submit the compliance report under subregulation (1) to the Cabinet.

(3) The annual compliance report shall be published on the official website of the Office.

50. Reports by data collector, data processor, data controller

Every data collector, data processor and data controller registered under these Regulations, shall within ninety days after the end of every financial year, submit to the Office a summary of—

(a) all complaints received and the status of such complaints, including whether the complaint was resolved or is still pending; and

(b) all data breaches and the action taken to address such data breaches.

SCHEDULE 1

Regulation 10(5), 23(3)

FORM 1

NOTICE OF OBJECTION TO COLLECTION/PROCESSING OF PERSONAL DATA

I, ... *(insert full name and address of data subject),* wish to withdraw my consent for the collection/processing *(whichever is applicable)* of the personal data provided to the Data Collector/ Data Processor/Data Controller *(whichever is applicable)* for:

- All the purposes I had provided my consent for; or
- For only the following purposes .....

  State purpose of objection to collection/processing of personal data.....

I fully understand and agree that the withdrawal of my consent to any or all purposes, depending on the nature of my request, may result in the Data Collector/ Data Processor/Data Controller, not being in a position to continue to provide services to me.

Date of application.....

Signature of data subject.....

FORM 2

APPLICATION FOR REGISTRATION/RENEWAL OF REGISTRATION

To: The Personal Data Protection Office
Kampala

APPLICATION FOR REGISTRATION/RENEWAL OF REGISTRATION

Data Collector/Data Processor/Data Controller
(*tick whichever is applicable*)

1. Details of applicant

   (a) Name of applicant[1] .....

   (b) Physical address of applicant .....

   (c) Telephone No/Email/Fax/ of applicant .....

   (d) Nature of business of applicant.....

2. Details of data protection officer

   (a) Name of Data Protection Officer.....

   (b) Physical address of Data Protection Officer .....

   (c) Telephone No/Email/Fax/ of Data Protection Officer .....

   (d) Please state whether Data Protection Officer has other duties in the Institution, public body or corporation, and if any, provide details.....

3. Description of data to be collected or processed (*be detailed as possible*) .....

4. Description of purpose for which data is collected or processed[2] (*be detailed as possible*) .....

1 If you are an individual or sole trader, give your surname and first name(s). A partnership must include the name of the firm and the names of each of the partners. In the case of a corporation, the name of the corporation must be given.

2 Please provide a general, but comprehensive, statement of the nature of your business, trade or profession, and of the purpose for which you keep and process personal data.
NOTE: Please note that where personal data is kept for two or more purposes, a separate application for registration in respect of any of those purposes must be made as per section 29(2) of the Act.

5. List persons or bodies to whom personal data may be disclosed and purpose for disclosure[3].....

6. List countries data may be transferred to, purpose of transfer and brief description of data transferred[4].....

7. State security measures in place to safeguard data collected or processed .....

8. Duration for which data shall be kept.....
.....

9. Attach written undertaking not to process or store personal data in a country outside Uganda unless such country has adequate measures in place, at least equivalent to the protection provided for by the Act, for the protection of the personal data and the data subject consent to the transfer.

10. Any other information required by the Office .....

I certify that the above information is correct and complete and hereby apply to be registered as data collector/data processor/data controller under the Data Protection and Privacy Act.

Signature of Applicant: .....

Date: .....
(*Applicant/Person authorised to sign on behalf of Applicant) *(*Delete whichever is not applicable*)

NOTES:

1. It is important that you read "Registration Classification and Guidance Notes for Application" before completing this form.

1. Use this form if you are a data collector, data processor or data controller who is required to be registered under the Data Protection and Privacy Act.

3

4 For each application listed, list the countries or territories (if any) to which you transfer, or intend to transfer, personal data directly or indirectly, along with a description of the data to be transferred and the purpose of transfer.

2. Please complete this form in BLOCK CAPITALS.

3. Failure to register or renew registration is an offence under the Data Protection and Privacy Act, 2019.

4. Knowingly giving false information is an offence under the Data Protection and Privacy Act.

5. It is also an offence to knowingly—

   (a) keep personal data not specified on your applications,

   (b) keep or use personal data for any purpose, or disclose personal data to any person or body, not described in those applications or

   (c) transfer personal data to a country or territory not permitted by the Office.

6. Where you change your address, you must notify the Office within 15 days of the change of address.

7. The information provided by you in this application will be kept in a register by the Director, in accordance with section 29 of the Data Protection and Privacy Act, 2019 and will comprise the Register which may be inspected by members of the public at any time.

Regulation 16(4)

FORM 3

UNDERTAKING NOT TO PROCESS OR STORE PERSONAL DATA OUTSIDE UGANDA

I, ... *(insert full name and address of applicant)* undertake not to process or store personal data in a country outside Uganda unless such country has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by the Act or permitted under the Act and Regulations made under the Act.

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

Signature of person making undertaking

Declared on this ..... day of ....., 20 ....., at .....

.....
(state place)

.....
Signature of person making undertaking

Before me

.....
Commissioner for Oaths

FORM 4

CERTIFICATE OF REGISTRATION

I CERTIFY THAT ..... (*insert name of company, individual or public body) has this day been registered as*

..... (*insert category: data collector/data processor/ data controller*) under the Data Protection and Privacy Act, 2019 under the following registration number.....

This certificate is valid for twelve months from the date of issue.

Dated this.....day of.....the year.....

.....

National Personal Data Protection Director

Regulation 28(3)

FORM 5

APPLICATION FOR CERTIFIED COPY OF EXTRACT/ENTRY IN REGISTER

Record of Copy of Extract/Entry in Register.....

Registration Particulars:

Date.....

Registration Number.....

Purpose of Extract/Entry in Register

Date of Application.....

Particulars of Applicant: .....

Name.....

Telephone Number.....

E-Mail Address.....

Place of work/Address.....

Comments by Records Officer.....

Comments by Office.....

Date of application: .....

Signature of Applicant.....

FORM 6

COMPLAINT CONCERNING PROCESSING PERSONAL DATA WITHOUT APPROPRIATE SECURITY MEASURES

DETAILS OF PERSON MAKING COMPLAINT	
First Name:	
Last Name:	
Address:	
E-mail address:	
Phone Number:	
DETAILS OF COMPLAINT	
My complaint is against: (*name of person, institution, or public body against whom complaint is being made*)	
Address of person making complaint: (*please provide full address of person making complaint*)	
I have been dealing with: (*institution, or public body against whom complaint is being made*)	
Date:	
Nature of complaint (*provide full details of complaint*)	

Date .....

Signature of person making complaint: .....

FORM 7

NOTIFICATION OF DATA BREACH

1. Details of person making notification

First Name:	
Last Name:	
Address:	
E-mail address:	
Phone Number:	

2. Details of Data Breach

a)	When did the breach happen?
b)	How did the breach happen?
c)	If there has been a delay in reporting the breach please explain the reasons for this
d)	What measures were in place to prevent an breach of this nature occurring?
e)	Please provide extracts from any policies or procedures considered relevant to this breach, and explain which of these were in existence at the time of this breach. Please provide the dates on which they were implemented.

Personal data placed at risk

f)	What personal data has been placed at risk? Please specify if any financial or sensitive personal data (special categories*) has been affected and provide details of the extent.
g)	How many data subjects have been affected and how many data records are involved?
h)	Are the affected individuals aware that the breach has occurred?
i)	What are the potential consequences and adverse effects on those individuals?
j)	Have any affected individuals complained to the University about the breach?

Containment and recovery

k) Has any action been taken to minimise/mitigate the effect on the affected data subjects? If so, please provide details.
l) Has the data placed at risk now been recovered? If so, please provide details of how and when this occurred.
m) What steps have been taken to prevent a recurrence of this breach?

Miscellaneous

n) Have the police or any other regulatory bodies been informed about this breach?
o) Has there been any media coverage of the breach?

* Special Categories of Personal data include:

- ☐ The racial or ethnic origin of the data subject
- ☐ Their political opinions
- ☐ Their religious or philosophical beliefs
- ☐ Whether they are a member of a trade union
- ☐ Their genetic data
- ☐ Biometric data used to uniquely identify them
- ☐ Their physical or mental health or condition
- ☐ Their sex life or sexual orientation

Date .....

Signature of person making notification: .....

Regulation 35(1)

FORM 8

REQUEST TO CONFIRM POSSESSION OF PERSONAL DATA

1. Name of data subject: .....

2. Data subjects National Identification Number/Passport/Driver's License/Aliens Identification card: .....

3. Data subject's email: .....

4. Data subject's phone number(s): .....

5. Name of the data processor/controller from whom information is being requested:

   .....

   .....

6. Description of personal data on data subject held by data processor/ controller (*include the categories of data, purposes of processing data, third parties the personal data may have disclosed to period for which the data has been held*): .....

7. Relevant period of information: .....

   from: ..... to: .....

8. Preferred form of access:
   hard copy/ soft copy (tick appropriately)
   (*Attach further details in an attached separate sheet, if necessary*)

   Date of request:.....

   Signature: .....
   (*signature of data subject or person authorised to act on behalf data subject*)

FORM 9

COMPLAINT CONCERNING INACCURATE PERSONAL DATA IN THE POSSESSION OF DATA CONTROLLER

DETAILS OF PERSON MAKING COMPLAINT	
First Name:	
Last Name:	
Address:	
E-mail address:	
Phone Number:	
DETAILS OF COMPLAINT	
My complaint is against: (*name of person, institution, or public body against whom complaint is being made*)	
Address of person making complaint: (*please provide full address of person making complaint*)	
I have been dealing with: (*institution, or public body against whom complaint is being made*)	
Date:	
Nature of complaint (*provide full details of complaint*)	

Date: .....

Signature: .....

Regulation 39(5)

FORM 10

DECISION ON COMPLAINT IN RESPECT OF INACCURATE PERSONAL DATA IN THE POSSESSION OF DATA CONTROLLER

TO: .....
(insert details of person making complaint)

Having reviewed your complaint lodged with the Personal Data Protection Office on ..... day of ..... 20..., concerning ..... (*insert brief details relating to complaint*) the decision of the Office is as follows:

.....
(*insert details of decision*)

Date of Decision:.....

.....
National Personal Data Protection Director

FORM 11

COMPLAINT CONCERNING INFRINGEMENT OR VIOLATION OF THE ACT

DETAILS OF PERSON MAKING COMPLAINT	
First Name:	
Last Name:	
Address:	
E-mail address:	
Phone Number:	
DETAILS OF COMPLAINT	
My complaint is against: (*name of person, institution, or public body against whom complaint is being made*)	
Address of person making complaint: (*please provide full address of person making complaint*)	
I have been dealing with: (*institution, or public body against whom complaint is being made*)	
Date:	
Nature of complaint (*provide full details of complaint*)	

Date: .....

Signature: .....

Regulation 45(2)

FORM 12

DECISION OF THE OFFICE ON COMPLIANT CONCERNING INFRINGEMENT OR VIOLATION OF THE ACT

TO: .....
(insert details of person making complaint)

Having reviewed your complaint lodged with the Personal Data Protection Office on ..... day of ..... 20....., concerning ..... (*insert brief details relating to complaint*) the decision of the Office is as follows:

..... (*insert details of decision*)

Date of Decision.....

.....
National Personal Data Protection Director

FORM 13

APPEAL

TO: PERMANENT SECRETARY OF MINISTRY FOR INFORMATION AND COMMUNICATIONS TECHNOLOGY

APPEAL

.....

..... *(insert name)* being dissatisfied with the decision of the Personal Data Protection Office made on the ..... day of ..... 20..... in respect of ..... (*insert decision of the Personal Data Protection Office and copy of the decision*) hereby apply to the Minister to review the decision.

The reasons for the appeal are as follows:

(a) .....

(b) .....

(c) .....

(d) .....

(e) .....

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

.....

Name and signature of person appealing

(*insert name and designation of the person making application*)

FORM 14

DECISION OF MINISTER

TO: .....
(insert details of person making the appeal)

DECISION OF MINISTER ON APPEAL

Having reviewed your appeal, lodged with the Ministry responsible for Information and Communications Technology on ..... day of ..... 20..., my decision is as follows:

.....

.....
(*insert details of decision*)

Date of Decision:.....

.....
Minister of Information and Communications Technology

SCHEDULE 2

Regulation 16(1), 28(2),

FEES

No.	*Description of fee*	*Uganda Shillings*
1.	Application for registration	100,000/=
2.	Application for renewal of registration	100,000/=
3.	Certified copy of an extract or entry in the Register (one copy)	25,000/=

JUDITH NABAKOOBA (MP),
Minister of Information Communications and Telecommunications and National Guidance.

Printed by Uganda Printing and Publishing Corporation