THE REPUBLIC OF UGANDA

THE DATA PROTECTION AND PRIVACY ACT, 2019

Act No. 9 of 2019

ACTS
SUPPLEMENT No. 6 3rd May, 2019.

ACTS SUPPLEMENT

to The Uganda Gazette No. 21, Volume CXII, dated 3rd March, 2019.

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

Act 9 *Data Protection and Privacy Act* **2019**

THE DATA PROTECTION AND PRIVACY ACT, 2019.

ARRANGEMENT OF SECTIONS

Section

PART I—PRELIMINARY

1. Application.
2. Interpretation.

PART II—PRINCIPLES OF DATA PROTECTION

3. Principles of data protection.

PART III—DATA COLLECTION AND PROCESSING

4. Establishment of the personal data protection office
5. Functions of the personal data protection office
6. Data protection officer
7. Consent to collect or process personal data
8. Personal data relating to children
9. Prohibition on collection and processing of special personal data
10. Protection of privacy
11. Collection of data from data subject.
12. Collection of personal data for specific purpose
13. Information to be given to data subject before collection of data
14. Minimality
15. Quality of information
16. Correction of personal data
17. Further processing to be compatible with purpose of collection
18. Retention of records of personal data
19. Processing personal data outside Uganda

PART IV—SECURITY OF DATA

20. Security measures
21. Security measures relating to data processed by data processor

Section

22. Data processed by operator or authorised person
23. Notification of data security breaches

PART V—RIGHTS OF DATA SUBJECTS

24. Right to access personal information
25. Right to prevent processing of personal data
26. Right to prevent processing of personal data for direct marketing
27. Rights in relation to automated decision-taking
28. Rectification, blocking, erasure and destruction of personal data

PART VI—DATA PROTECTION REGISTER

29. Data protection register
30. Access to register by the public

PART VII—COMPLAINTS

31. Complaints against breach and non-compliance
32. Authority to investigate complaints
33. Compensation for failure to comply with this Act
34. Appeals

PART VIII—OFFENCES

35. Unlawful obtaining or disclosing of personal data.
36. Unlawful destruction, deletion, concealment or alteration of personal data.
37. Sale of personal data
38. Offences by corporations.
39. Regulations
40. Power of the Minister to amend Schedule

Schedule
Currency point

THE DATA PROTECTION AND PRIVACY ACT, 2019

An Act to protect the privacy of the individual and of personal data by regulating the collection and processing of personal information; to provide for the rights of the persons whose data is collected and the obligations of data collectors, data processers and data controllers; to regulate the use or disclosure of personal information; and for related matters.

DATE OF ASSENT: 25th February, 2019.

Date of Commencement: 3rd May, 2019

BE IT ENACTED by Parliament as follows:

PART I—PRELIMINARY

1. Application.

This Act applies to a person, institution or public body—

(a) collecting, processing, holding or using personal data within Uganda;

(b) outside Uganda who collects, processes, holds, or uses personal data relating to Ugandan citizens.

2. Interpretation.

In this Act unless the context otherwise requires—

"Authority" means the National Information Technology Authority – Uganda;

"consent" means any freely given, specific, informed and unambiguous indication of the data subject's wish which he or she, by a statement or by a clear affirmative action, signifies agreement to the collection or processing of personal data relating to him or her;

"corporation" means an entity created under a law and is separate and distinct from its owners;

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

"data" means information which—

(a) is processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should be processed by means of such equipment;

(c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system; or

(d) does not fall within paragraph (a),(b) or (c) but forms part of an accessible record;

"data collector" means a person who collects personal data;

"data controller" means a person who alone, jointly with other persons or in common with other persons or as a statutory duty determines the purposes for and the manner in which personal data is processed or is to be processed;

"data processor" in relation to personal data, means a person other than an employee of the data controller who processes the data on behalf of the data controller;

"data subject" means an individual from whom or in respect of whom personal information has been requested, collected, collated, processed or stored;

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

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

"personal data" means information about a person from which the person can be identified, that is recorded in any form and includes data that relates to—

(a) the nationality, age or marital status of the person;

(b) the educational level, or occupation of the person;

(c) an identification number, symbol or other particulars assigned to a person;

(d) identity data; or

(e) other information which is in the possession of, or is likely to come into the possession of the data controller and includes an expression of opinion about the individual;

"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 any such 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 the 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 the benefit, regulation and control of any profession;

"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;

"recipient" means a person to whom data is disclosed including an employee or agent of the data controller or the data processor to whom data is disclosed in the course of processing the data for the data controller, but does not include a person to whom disclosure is made with respect to a particular inquiry pursuant to an enactment;

"third party" in relation to personal data, means a person other than the data subject, the data collector, data controller, or any data processor or other person authorised to process data for the data controller or processor.

PART II—PRINCIPLES OF DATA PROTECTION

3. Principles of data protection.

(1) A data collector, data processor or data controller or any person who collects, processes, holds or uses personal data shall—

(a) be accountable to the data subject for data collected, processed held or used;

(b) collect and process data fairly and lawfully;

(c) collect, process, use or hold adequate, relevant and not excessive or unnecessary personal data;

(d) retain personal data for the period authorised by law or for which the data is required;

(e) ensure quality of information collected, processed, used or held;

(f) ensure transparency and participation of the data subject in the collection, processing, use and holding of the personal data; and

(g) observe security safeguards in respect of the data.

(2) The Authority shall ensure that every data collector, data controller, data processor or any other person collecting or processing data complies with the principles of data protection and this Act.

4. Establishment of the personal data protection office.

(1) There is established a personal data protection office responsible for personal data protection under the Authority which shall report directly to the Board.

(2) The personal data protection office established in subsection (1) 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.

(3) The national personal data protection director shall be a person of high moral character, proven integrity and with the relevant qualifications and experience relating to the functions of the office.

(4) The personal data protection office shall consist of such other officers as may be necessary for the proper functioning of the office appointed on such terms and conditions as may be specified in the instruments of appointment.

5. Functions of the personal data protection office.

(1) For purposes of this Act and in addition to its functions under any other law, the personal data protection office shall—

(a) oversee the implementation of and be responsible for the enforcement of this Act;

(b) promote the protection and observance of the right to the privacy of a person and of personal data;

(c) monitor, investigate and report on the observance of the right to privacy and of personal data;

(d) formulate, implement and oversee programmes intended to raise public awareness about this Act;

(e) receive and investigate complaints relating to infringement of the rights of the data subject under this Act;

(f) establish and maintain a data protection and privacy register;

(g) perform such other functions as may be prescribed by any other law or as the office considers necessary for the promotion, implementation and enforcement of this Act;

(2) The office shall have all powers necessary for the performance of its functions under this Act.

(3) The office in performing its functions under this Act shall not be under the direction or control of any person or Authority.

6. Data protection officer.

For purposes of this Act, and in so far as it applies to an institution, the head of the institution shall designate a person as the data protection officer responsible for ensuring compliance with this Act.

PART III—DATA COLLECTION AND PROCESSING

7. Consent to collect or process personal data.

(1) Subject to subsection (2), a person shall not collect or process personal data without the prior consent of the data subject.

(2) Personal data may be collected or processed—

(a) where the collection or processing is authorised or required by law; or

(b) where it is necessary—

(i) for the proper performance of a public duty by a public body;

(ii) for national security;

(iii) for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law.

(c) for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(d) for medical purposes; or

(e) for compliance with a legal obligation to which the data controller is subject.

(3) Except for data collected or processed under subsection (2), where a data subject objects to the collection or processing of personal data, the person who is collecting or processing the personal data shall stop the collection or processing of the personal data.

8. Personal data relating to children.

A person shall not collect or process personal data relating to a child unless the collection or processing thereof is;

(a) carried out with the prior consent of the parent or guardian or any other person having authority to make decisions on behalf of the child;

(b) necessary to comply with the law; or

(c) for research or statistical purposes.

9. Prohibition on collection and processing of special personal data.

(1) A person shall not collect or process personal data which relates to the religious or philosophical beliefs, political opinion, sexual life, financial information, health status or medical records of an individual.

(2) This section does not apply to information collected under the Uganda Bureau of Statistics Act.

(3) A data collector, data processor and data controller may collect or process personal data specified under subsection(1) where—

(a) the collection or processing of the data is in the exercise or performance of a right or an obligation conferred or imposed by law on an employer;

(b) the information is given freely and with the consent of the data subject; or

(c) the collection or processing of the information is for the purposes of the legitimate activities of a body or association which—

(i) is established for non-profit purposes; or

(ii) exists for political, philosophical, religious or trade union purposes; and

(iii) relates to individuals who are members of the body or association or have regular contact with the body or association in connection with its purposes, and does not involve disclosure of the personal data to a third party without the consent of the data subject.

10. Protection of privacy.

A data collector, data processor or data controller shall not collect, hold or process personal data in a manner which infringes on the privacy of a data subject.

11. Collection of data from data subject.

(1) A person shall collect personal data directly from the data subject.

(2) Notwithstanding subsection (1), personal data may be collected from another person, source or public body where—

(a) the data is contained in a public record;

(b) the data subject has deliberately made the data public;

(c) the data subject has consented to the collection of the information from another source;

(d) the collection of the data from another source is not likely to prejudice the privacy of the data subject;

(e) the collection of the data from another source is necessary—

(i) for the prevention, detection, investigation, prosecution or punishment of an offence or breach of law;

(ii) for the enforcement of a law which imposes a pecuniary penalty;

(iii) for the enforcement of legislation which concerns public revenue collection;

(iv) for the conduct of proceedings before any court or tribunal that have commenced or are reasonably contemplated; or

(v) for the protection of national security;

(f) compliance would prejudice a lawful purpose for the collection; or

(g) it is not reasonably practicable to obtain the consent of the data subject.

12. Collection of personal data for specific purpose.

A person who collects personal data shall collect the data for a lawful purpose which is specific, explicitly defined and is related to the functions or activity of the data collector, or data controller.

13. Information to be given to data subject before collection of data.

(1) A person collecting personal data shall inform the data subject about—

(a) the nature and category of data being collected;

(b) the name and address of the person responsible for the collection of data;

(c) the purpose for which the data is required;

(d) whether or not the supply of the data by the data subject is discretionary or mandatory;

(e) the consequences of failure to provide the data;

(f) the authorised requirement for the collection of the information or the requirement by law for its collection;

(g) the recipients of the data;

(h) the existence of the right of access to and the right to request rectification of the data collected before the collection; and

(i) the period for which the data will be retained to achieve the purpose for which it is collected.

(2) Where the data is collected from a third party, the data subject shall be given the information specified in subsection (1) before the collection of the data or as soon as practicable after the collection of the data.

(3) Subsection (2) shall not apply—

(a) where it is necessary to avoid the compromise of the law enforcement power of a public body responsible for the prevention, detection, investigation, prosecution or punishment of an offence;

(b) to information relating to national security;

(c) to information relating to the enforcement of a law which imposes a pecuniary penalty;

(d) to information relating to the enforcement of legislation which concerns public revenue collection;

(e) to information relating to the preparation or conduct of proceedings before a court or tribunal.

14. Minimality.

(1) A data controller or data processer shall only process the necessary or relevant personal data.

(2) For the avoidance of doubt, a data controller or data processer shall not process personal data which is in excess of the data which is authorised by law or required for a specific purpose.

15. Quality of information.

(1) A data collector or data processor or data controller shall ensure that the data is complete, accurate, up-to-date and not misleading having regard to the purpose for its collection or processing.

(2) A data subject shall ensure that the personal data given to the data collector or data processor or data controller is complete, accurate, up to date and not misleading.

16. Correction of personal data.

(1) A data subject may request a data controller to—

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

(2) On receipt of the request, a data controller shall comply with the request.

(3) Where the data controller is not able to comply with the request under subsection (1), the data controller shall inform the data subject of the rejection, and the reasons for the rejection in writing.

(4) Where the data controller complies with the request, the data controller shall inform each person to whom the personal data has been disclosed of the correction made.

(5) The data controller shall notify the data subject of the action taken as a result of the request.

17. Further processing to be compatible with purpose of collection.

(1) Where a person holds personal data collected in connection with a specific purpose, further processing of the personal data shall only be for that specific purpose.

(2) For the purposes of subsection (1), a person who processes personal data under this section shall take into account—

(a) the relationship between the purpose of the intended further processing and the purpose for which the data was collected;

(b) the nature of the data concerned;

(c) the manner in which the data has been collected;

(d) the consequences that the further processing is likely to have for the data subject; and

(e) the contractual rights and obligations between the data subject and the person who processes the data.

(3) The further processing of data is considered to be compatible with the purpose of collection where—

(a) the data subject consents to the further processing of the information;

(b) the data is publicly available or has been made public by the person concerned;

(c) further processing is necessary—

(i) for the prevention, detection, investigation, prosecution or punishment for an offence or breach of law;

(ii) for the enforcement of a law which imposes a pecuniary penalty;

(iii) for the enforcement of legislation that concerns protection of public revenue collection;

(iv) for the conduct of proceedings before any court or tribunal that have commenced;

(v) for the protection of national security; or

(vi) to prevent or mitigate a serious and imminent threat to public health or safety or the life or health of the data subject or another individual;

(d) the data is used for historical, statistical or research purposes and the person responsible for the processing ensures that—

(i) the further processing is carried out solely for the purpose for which the data was collected; and

(ii) that the data is not published in a form likely to reveal the identity of the data subject.

18. Retention of records of personal data.

(1) Subject to subsections (2) and (3), a person who collects personal data shall not retain the personal data for a period longer than is necessary to achieve the purpose for which the data is collected and processed unless—

(a) the retention of the data is required or authorised by law;

(b) the retention of the data is necessary for a lawful purpose related to a function or activity for which the data is collected or processed;

(c) the retention of the data is required by a contract between the parties to the contract; or

(d) the data subject consents to the retention of the data.

(2) Subsection (1) does not apply to personal data retained for—

(a) the prevention, detection, investigation, prosecution or punishment of an offence or breach of law;

(b) the national security purposes;

(c) the enforcement of a law which imposes a pecuniary penalty;

(d) the enforcement of legislation relating to public revenue collection;

(e) the conduct of proceedings before any court or tribunal ; or

(f) historical, statistical, or research purposes.

(3) A person who uses personal data of a data subject to make a decision about the data subject shall—

(a) retain the data for a period required or prescribed by law; or

(b) where no retention period is required by law, retain the data for a period which shall afford the data subject an opportunity to request access to the data.

(4) A data controller shall destroy or delete a record of personal data or de-identify the record at the expiry of the retention period.

(5) The destruction or deletion of a record of personal data shall be done in a manner that prevents its reconstruction in an intelligible form.

19. Processing personal data outside Uganda.
Where a data processor or data controller based in Uganda processes or stores personal data outside Uganda, the data processor or data controller shall ensure that—

(a) the country in which the data is processed or stored has adequate measures in place for the protection of personal data at least equivalent to the protection provided for by this Act; or

(b) the data subject has consented.

PART IV—SECURITY OF DATA

20. Security measures.

(1) A data controller, data collector or data processor shall secure the integrity of personal data in the possession or control of a data controller, data processor or data collector by adopting appropriate, reasonable, technical and organisational measures to prevent loss, damage, or unauthorised destruction and unlawful access to or unauthorised processing of the personal data.

(2) For the purposes of subsection (1), the data controller shall take measures to—

(a) identify reasonably foreseeable internal and external risks to personal data under that person's possession or control;

(b) establish and maintain appropriate safeguards against the identified risks;

(c) regularly verify that the safeguards are effectively implemented; and

(d) ensure that the safeguards are continually updated in response to new risks or deficiencies.

(3) A data controller shall observe generally accepted information security practices and procedures, and specific industry or professional rules and regulations.

21. Security measures relating to data processed by data processor.

(1) A data controller shall not permit a data processor to process personal data for the data controller, unless the data processor establishes and complies with the security measures specified under this Act.

(2) A contract between a data controller and a data processor relating to processing of personal data, shall require the data processor to establish and maintain the confidentiality and security measures necessary to protect the integrity of the personal data.

22. Data processed by operator or authorised person.

(1) An operator or a person who processes personal data on behalf of a data controller shall process the data only with the prior knowledge or authorisation of the data controller and shall treat the personal data which comes to the knowledge of the operator or other person as confidential.

(2) A data processor shall not disclose the data unless required by law, or in the course of the discharge of a duty.

23. Notification of data security breaches.

(1) Where a data collector, data processor or data controller, believes that the personal data of a data subject has been accessed or acquired by an unauthorised person, the data collector, data processor or data controller, shall immediately notify the Authority in the prescribed manner, of the unauthorised access or acquisition and the remedial action taken.

(2) The Authority shall determine and notify the data controller, data collector or data processor whether the data controller, data collector or data processor should notify the data subject of the breach.

(3) Where the Authority determines that the data collector, data processor or data controller should notify the data subject, the notification shall be made by—

(a) registered mail to the data subject's last known residential or postal address;

(b) electronic mail to the data subject's last known electronic mail address;

(c) placement in a prominent position on the website of the responsible party; or

(d) publication in the mass media.

(4) A notification referred to in sub section (3) shall provide sufficient information relating to the breach to allow the data subject to take protective measures against the consequences of unauthorised access or acquisition of the data.

(5) Where the Authority has grounds to believe that publicity would protect a data subject who is affected by the unauthorised access or acquisition of data, the Authority shall direct the responsible party to publicise in the specified manner, the fact of the compromise to the integrity or confidentiality of the personal data.

PART V—RIGHTS OF DATA SUBJECTS

24. Right to access personal information

(1) A data subject who provides proof of identity may request a data controller to—

(a) confirm whether or not the data controller holds personal data about that data subject;

(b) give a description of the personal data which is held by the data controller;

(c) provide the identity of a third party or a category of a third party who has or has had access to information.

(2) A request under this section shall be made in the prescribed form and manner.

(3) A data controller shall not comply with a request under this section unless the data controller is given information that the data controller may reasonably require to identify the person making the request and to locate the data requested by that person.

(4) Where a data controller is unable to comply with the request without disclosing data related to another individual who may be identified from the information, the data controller shall not comply with the request unless—

(a) the other individual consents to the disclosure of the data to the person who makes the request;

(b) it is reasonable in all the circumstances to comply with the request without the consent of the other individual; or

(c) compelled by a court order.

(5) For the purposes of subsection (4)—

(a) a reference to data related to another individual includes a reference to data which identifies that individual as the source of the data requested; and

(b) another individual may be identified from the data disclosed if that individual can be identified from that data, or any other data which in the reasonable belief of the data controller are likely to be in, or come into the possession of the data subject who made the request.

(6) A data controller shall not use subsection (4) as an excuse for failing to communicate so much of the information sought that may be communicated without the disclosure of the identity of the individual concerned.

(7) The data controller may make the communication under subsection (6) by omitting or deleting the name or other identifying particulars of the other individual.

(8) For the purposes of subsection (4), to determine whether it is reasonable to comply with the request without the consent of the other individual concerned, the data controller shall take into account—

(a) any duty of confidentiality owed to the other individual;

(b) any steps taken by the data controller to seek the consent of that other individual;

(c) whether the other individual is capable of giving consent; and

(d) any express refusal of consent by the other individual.

(9) Subject to subsection (4), a data controller shall comply with a request under this section promptly and in any event within thirty days from the date of receipt of the request.

25. Right to prevent processing of personal data.

(1) A data subject shall at any time by notice in writing to a data controller or data processor, require the data controller or data processor to stop processing personal data which causes or is likely to cause unwarranted substantial damage or distress to the data subject.

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

(3) Where the data controller gives reasons for non-compliance, a copy of the notice required by subsection (2) shall be given to the Authority within fourteen days.

(4) Where the Authority is satisfied that the data subject is justified, the Authority shall direct the data controller to comply within seven days.

(5) This section does not apply to data collected or processed in accordance with section 7(2).

26. Right to prevent processing of personal data for direct marketing.

(1) A data subject may by notice in writing to a data controller, require the data controller to stop processing his or her personal data for purposes of direct marketing.

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

(3) Subject to sub-section (1) a data subject may enter into agreement with a data controller for purposes of using or processing his or her personal data for pecuniary benefits.

(4) Where the data controller gives reasons for non-compliance, a copy of the notice required by subsection (2) shall be given to the Authority within the time specified in that subsection.

(5) Where the Authority is satisfied that the notice in subsection (1) is justified, the Authority may direct the data controller to comply.

(6) In this section "direct marketing" includes the communication by whatever means of any advertising or marketing material which is directed at an individual.

27. Rights in relation to automated decision-taking.

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

(2) Without prejudice to subsection (1), where a decision which significantly affects a data subject is based solely on automated processing—

(a) the data controller shall as soon as reasonably practicable notify the data subject that the decision was taken on that basis, and

(b) the data subject is entitled, by notice in writing to require the data controller to reconsider the decision within twenty-one days after receipt of the notification from the data controller.

(3) The data controller shall, within twenty-one days after receipt of the notice, inform the data subject in writing of the steps that the data controller has taken to comply with the notice.

(4) This section does not apply to a decision made—

(a) in the course of considering whether to enter into a contract with the data subject;

(b) with a view to entering into the contract;

(c) in the course of the performance of the contract; or

(d) for a purpose authorised or required by or under any law

(5) Where the data subject is not satisfied with the decision of the data controller in subsection (3), the data subject shall complain in writing to the Authority within fourteen days.

(6) Where the Authority is satisfied on a complaint by a data subject that the data controller has failed to comply, the Authority shall order the data controller to comply within seven days.

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

(1) Where the Authority is satisfied on a complaint of a data subject that personal data on that data subject is inaccurate, the Authority may order the data controller to rectify, update, block, erase, or destroy the data.

(2) Subsection (1) applies whether the data is an accurate record of information received or obtained by the data controller from the data subject or a third party.

(3) Where the data is an inaccurate record of the information, the Authority may direct the data controller to update the statement of the true facts which the Authority considers appropriate.

(4) Where the data complained of has been rectified, blocked, updated, erased or destroyed, the data controller is required to notify third parties to whom the data has been previously disclosed of the rectification, blocking, updated, erasure or destruction.

PART VI—DATA PROTECTION REGISTER

29. Data protection register.

(1) The Authority shall keep and maintain a data protection register.

(2) The Authority shall register in the data protection register, every person, institution or public body collecting or processing personal data and the purpose for which the personal data is collected or processed.

(3) An application by a data controller or other person to register shall be made in the prescribed manner.

30. Access to register by the public.
The Authority shall make the information contained in the Data Protection Register available for inspection by any person.

PART VII—COMPLAINTS.

31. Complaints against breach and non-compliance.
(1) A data subject or any person who believes that a data collector, data processor or data controller is infringing upon their rights or is in violation of this Act may make a compliant in the prescribed manner to the Authority.

(2) A data collector, data processor or data controller may in writing make a complaint to the Authority about any violation or non-compliance with this Act.

32. Authority to investigate complaints.
The Authority shall investigate every compliant made under this Part and may direct a data collector, data processor or data controller to remedy any breach or take such action as the Authority may specify to restore the integrity of data collected, processed or held by the data collector, data processor or data controller or the rights of the data subject.

33. Compensation for failure to comply with this Act.
(1) Where a data subject suffers damage or distress through the contravention by a data controller, data processor or data collector of the requirements of this Act, that data subject is entitled to apply to a Court of competent jurisdiction for compensation from the data collector, data processor or data controller for the damage or distress.

(2) In proceedings against a person under this section, it is a defence to prove that the person took reasonable care in all the circumstances to comply with the requirements of this Act.

34. Appeals.
(1) A person aggrieved by a decision of the Authority under this Act may appeal to the Minister.

(2) The appeal shall be made within thirty days from the date of notice of the decision.

(3) A copy of the appeal shall be provided to the Authority.

PART VIII—OFFENCES

35. Unlawful obtaining or disclosing of personal data.

(1) A person shall not unlawfully obtain, disclose or procure the disclosure to another person of personal data held or processed by a data collector, data controller or data processor.

(2) A person who contravenes this section commits an offence and is liable on conviction to a fine not exceeding two hundred and forty currency points or imprisonment for ten years or both.

36. Unlawful destruction, deletion, concealment or alteration of personal data.

(1) A person shall not unlawfully destroy, delete, mislead, conceal or alter personal data.

(2) A person who contravenes this section commits an offence and is liable on conviction to a fine not less than two hundred and forty currency points or imprisonment not exceeding ten years or both.

37. Sale of personal data.

(1) A person shall not sell or offer for sale personal data of any person.

(2) A person who contravenes subsection (1) commits an offence and is liable on conviction to a fine not exceeding two hundred and forty five currency points or imprisonment not exceeding ten years or both.

38. Offences by corporations.

(1) Where an offence under sections 35, 36 and 37 is committed by a corporation, the corporation and every officer of the corporation who knowingly and willfully authorises or permits the contravention commits the offence.

(2) A court which convicts a person under subsection (1) may, in addition to the punishment order the corporation, pay a fine not exceeding two percent of the corporation's annual gross turnover.

(3) A court shall take into consideration the gravity of the offence under subsection (1) and its impact in determining the fine to impose under subsection (2).

39. Regulations.

The Minister may, after consultation with the Authority by statutory instrument make regulations for—

(a) any matter which is required to be prescribed;

(b) any administrative or procedural matter which is necessary to give effect to this Act;

(c) the retention period of personal data; or

(d) any matter which is necessary and expedient to give effect to this Act.

40. Power of the Minister to amend Schedule.

The Minister may, with the approval of Cabinet, by statutory instrument, amend the Schedule.

SCHEDULE

Currency point

One currency point is equivalent to twenty thousand shillings