ISSN 0856 - 034X

THE UNITED REPUBLIC OF TANZANIA

Supplement No. 21 ***13th JUNE, 2023***

SPECIAL SUPPLEMENT

To The Special Gazette of the United Republic of Tanzania No. 15 Vol. 104 Dated 13th June, 2023
Printed by The Government Printer, Dodoma by Order of Government

GOVERNMENT NOTICE NO. 395B published on 13/6/2023

THE UNITED REPUBLIC OF TANZANIA

CHAPTER 44

ENGLISH VERSION

THE PERSONAL DATA PROTECTION ACT

[PRINCIPAL LEGISLATION]

This version of the Personal Data Protection Act, Chapter 44 has been translated into English Language, and is published pursuant to section 84(4) of the Interpretation of Laws Act, Chapter 1.

Dodoma,
13th June, 2023

ELIEZER MBUKI FELESHI
Attorney General

GN. NO. 395B (Contd)

CHAPTER 44

THE PERSONAL DATA PROTECTION ACT

ARRANGEMENT OF SECTIONS

Section *Title*

PART I
PRELIMINARY PROVISIONS

1. Short title.
2. Application.
3. Interpretation.
4. Objectives of Act.
5. Principles of personal data protection.

PART II
PERSONAL DATA PROTECTION COMMISSION

6. Establishment of Personal Data Protection Commission.
7. Functions of Commission.
8. Establishment of Board.
9. Functions of Board.
10. Committees of Board.
11. Appointment of Director General.
12. Tenure of office of Director General.
13. Staff of Commission.

PART III
REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

14. Registration of data controllers and data processors.
15. Register of data controllers and data processors.
16. Duration of registration.

GN. NO. 395B (Contd)

17. Inspection of registered particulars.
18. Deregistration.
19. Offences relating to registration.
20. Appeal relating to registration.
21. Registration of public institutions.

PART IV
COLLECTION, USE, DISCLOSURE AND RETENTION OF PERSONAL DATA

22. Collection of personal data.
23. Source and notification of personal data.
24. Accuracy of personal data.
25. Personal data to be used for intended purpose.
26. Limitations on disclosure of personal data.
27. Security of personal data.
28. Retention and disposal of personal data.
29. Correction of personal data.
30. Prohibition on processing of sensitive personal data.

PART V
TRANSBORDER DATA FLOW

31. Transfer of personal data to state with adequate data protection.
32. Transfer of personal data to state without adequate data protection.

PART VI
RIGHTS OF DATA SUBJECTS

33. Right of access to personal data.
34. Right to prevent processing likely to affect data subject.
35. Right to prevent processing of personal data for direct marketing.
36. Rights in relation to automated decision making.
37. Right to compensation.
38. Rectification, blocking, erasure and destruction of personal data.

PART VII
INVESTIGATION OF COMPLAINTS

GN. NO. 395B (Contd)

39. Complaints against violation of personal data protection principles.
40. Notice of investigation.
41. Investigation confidentiality.
42. Powers of Commission in carrying out investigations.
43. Obstruction of Commission.
44. Seeking assistance of another person or authority.
45. Notice of enforcement.
46. Notice of penalty.
47. Administrative fines.
48. Review of decision.
49. Right of appeal.
50. Payment of compensation.

GN. NO. 395B (Contd)

PART VIII
FINANCIAL PROVISIONS

51. Sources of funds of Commission.
52. Financial management.
53. Estimates of income and expenditure and financial control.
54. Expenditure of funds.
55. Supplementary budget.
56. Accounts and audit.
57. Annual reports and performance agreements.

PART IX
MISCELLANEOUS PROVISIONS

58. Exceptions from application of provisions of this Act.
59. Preservation order.
60. Offences of unlawful disclosure of personal data.
61. Offences of unlawful destruction, deletion, concealment or alteration of personal data.
62. Offences by company or corporation.
63. General penalty.
64. Regulations.
65. Code of ethics for personal data protection.

GN. NO. 395B (Contd)

CHAPTER 44

THE PERSONAL DATA PROTECTION ACT

An Act to provide for principles of protection of personal data so as to establish minimum requirements for the collection and processing of personal data; to provide for establishment of Personal Data Protection Commission; to provide for improvement of protection of personal data processed by public and private bodies; and to provide for matters connected therewith.

[1st May, 2023]
[GN. NO. 326 of 2023]

Act No.
11 of 2022

PART I
PRELIMINARY PROVISIONS

Short title

1. This Act may be cited as the Personal Data Protection Act, 2022.

Application

2. This Act shall apply to Mainland Tanzania as well as Tanzania Zanzibar save that in Tanzania Zanzibar this Act shall not apply to non-union matters.

Interpretation

3. In this Act, unless the context otherwise requires-

"data protection officer" means an individual appointed by the data controller or data processor charged with ensuring compliance with the obligations provided for in this Act;

"code of ethics" means data-use charters which regulates

the conduct of a data controller or data processor prepared in accordance with section 65;

"court" means the court of competent jurisdiction;

"data processor" means a natural person, legal person or public body which processes personal data for and on behalf of the controller and under the data controller's instruction, except for the persons who, under the direct authority of the controller, are authorised to process the data and it includes his representative;

"data subject" means the subject of personal data which are processed under this Act;

"Director General" means the Director General of the Commission appointed under section 11;

"data controller" means a natural person, legal person or public body which alone or jointly with others determines the purpose and means of processing of personal data; and where the purpose and means of processing are determined by law, "data controller" is the natural person, legal person or public body designated as such by that law and it includes his representative;

"recipient" means a natural person, legal person, public body or any other person who receives personal data from a data controller;

"health professional" means a person providing health care services and recognised as such by the relevant law;

Cap. 13 "child" has the meaning ascribed to it under the Child Act;

"third party" means any natural or legal person, or public body other than-

(a) the data subject;

(b) the data controller or data processor; and

(c) any person who is authorised to process personal data;

"document" means any medium in which data is recorded, whether printed or on tape or film or by

electronic means or otherwise and includes any map, diagram, photograph, film, microfilm, video-tape, sound recording or machine-readable record or any record which is capable of being produced from a machine-readable record by means of equipment or a programme, or a combination of both, which is used by the data controller for record purposes;

"register" means the register established by the Commission under section 15;

"personal data" means data about an identifiable person that is recorded in any form, including-

(a) personal data relating to the race, national or ethnic origin, religion, age or marital status of the individual;

(b) personal data relating to the education, the medical, criminal or employment history;

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

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

(e) the name of the individual appearing on personal data of another person relating to the individual or where the disclosure of the name itself would reveal personal data about the individual;

(f) correspondence sent to a data controller by the data subject that is explicitly or implicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, and the views or opinions of any other person about the data subject;

"sensitive personal data" includes-

(a) genetic data, data related to children, data related to offences, financial transactions of the individual, security measure or biometric data;

(b) if they are processed for what they reveal,

personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, affiliation, trade-union membership, gender and data concerning health or sex life; and

(c) any personal data otherwise considered under the laws of the country as presenting a major risk to the rights and interests of the data subject;

"genetic data" means any personal data stemming from a Deoxyribonucleic acid (DNA) analysis;

"Commission" means the Personal Data Protection Commission established under section 6;

"processing" means analysis of personal data, whether or not by automated means, such as obtaining, recording or holding the data or carrying out any analysis on personal data, including:

(a) organization, adaptation or alteration of the personal data;

(b) retrieval or use of the data; or

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

"transborder flow" means any international cross-border flows of personal data by means of electronic transmission or other means;

"Minister" means the Minister responsible for communication.

Objectives of Act

4. The objectives of this Act are to-

(a) regulate the collection and processing of personal data;

(b) ensure that the collection and processing of personal data of a data subject is guided by the principles set out in this Act;

(c) protect the privacy of individuals;

(d) establish a legal and institutional mechanism to protect personal data; and

(e) provide data subjects with rights and

remedies to protect their personal data from collection and processing that is not in accordance with this Act.

Principles of personal data protection

5. A data controller or data processor shall ensure that personal data is-

(a) processed lawfully, fairly and transparently;

(b) collected for explicit, specified and legitimate purposes and not further processing in a manner incompatible with those purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed;

(d) accurate and where necessary, kept up to date, with every reasonable step taken to ensure that any inaccurate personal data is erased or rectified without delay;

(e) stored in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed;

(f) processed in accordance with the rights of a data subject;

(g) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against any loss, destruction or damage, using appropriate technical or organisational measures; and

(h) not transferred abroad contrary to the provisions of this Act.

PART II
PERSONAL DATA PROTECTION COMMISSION

Establishment of Personal Data Protection Commission

6.-(1) There is established a Commission to be known as the Personal Data Protection Commission.

(2) The Commission shall be a body corporate

GN. NO. 395B (Contd)

with perpetual succession and a common seal and, shall in its own name be capable of-

(a) acquiring and holding movable and immovable property, to dispose of property and to enter into any contract or other transaction;
(b) suing and being sued; and
(c) performing any other acts which a body corporate may lawfully perform, for the proper performance of its functions under this Act.

Functions of Commission

7. The functions of the Commission shall be to-

(a) monitor compliance by data controllers and data processors of the provisions of this Act;
(b) register data controllers and data processors in accordance with this Act;
(c) receive, investigate and deal with complaints about alleged violations of the protection of personal data and privacy of persons;
(d) inquire into and take measures against any matter, that appears to the Commission to affect the protection of personal data and infringe privacy of the individuals;
(e) educate the public as may be appropriate to the implementation of objectives of this Act;
(f) undertake research and to monitor technological developments in data processing;
(g) establish mechanisms of cooperation with other data protection authorities from other countries, and advise the Government on matters relating to implementation of this Act; and
(h) perform other functions of the Commission for better implementation of the provisions of this Act.

GN. NO. 395B (Contd)

Establishment of Board

8.-(1) There is hereby established a Board to be known as the Board of Personal Data Protection Commission which shall be the governing body of the Commission and shall consist of seven members as follows:

(a) a Chairman and Vice-Chairman; and

(b) five other members.

(2) The Chairman and the Vice-Chairman shall be appointed by the President on basis of the principle that where the Chairman hails from one part of the United Republic, the Vice-Chairman shall be a person who hails from the other part of the United Republic.

(3) The other five members under subsection (1)(b) shall be appointed by the Minister from among persons with qualification and experience in ICT, law, engineering, finance or administration.

(4) In order to maintain impartiality of the Commission and for the purpose of avoiding conflict of interest, a person shall not be qualified for appointment as a member of the Authority if owing to the nature of the office he holds, is likely to exert influence on the Commission.

(5) Director-General of Commission shall be the secretary to the Board.

(6) The provisions relating to the Board and its proceeding shall be as set out in the Schedule.

Functions of Board

9.-(1) The Board shall oversee the performance of the Commission so as to ensure adherence to the governing laws and procedures.

(2) Without prejudice to the generality of subsection (1), the Board shall-

(a) provide strategic guidance and formulate policies for operation and management of the Commission;

(b) conduct oversight on the activities and performance of management of the Commission;

GN. NO. 395B (Contd)

(c) ensure efficient use of resources, including approval of annual work plan, annual budget and supplementary budget;
(d) approve investment plans of the Commission;
(e) approve performance reports of the Commission;
(f) approve code of conduct for staff of Commission;
(g) approve and oversee financial regulations and staff rules;
(h) approve the disposal of assets of the Commission; and
(i) perform any other functions as it may consider necessary for the achievement of its goals in accordance with this Act.

Committees of Board

10. The Board may, for the purpose of efficient performance of its functions, form and appoint from among its members, such number of committees as it considers necessary.

Appointment of Director General

11.-(1) There shall be the Director General of the Commission who shall be appointed by the President.

(2) A person shall be qualified for appointment as Director General if he-

(a) is a graduate of a recognised university with a bachelor's degree or above in the fields of ICT, engineering, law, economics, finance or administration;
(b) has experience of not less than ten years of service in either of the fields referred in paragraph (a); and
(c) expresses knowledge and expertise in the field of personal data protection.

Tenure of office of Director General

12. The Director General shall hold office for a period of five years and may be reappointed for one further term.

Staff of Commission

13.-(1) The Commission shall, subject to the laws governing public service, employ other officers and employees of such number as may be necessary for the effective discharge of the functions of the Commission.

(2) The Commission may appoint consultants and experts in various disciplines on such terms and conditions as the Commission may determine.

PART III
REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Registration of data controllers and data processors

14.-(1) A person shall not collect or process personal data without being registered as a data controller or a data processor under this Act.

(2) A person who intends to collect or process personal data shall apply to the Commission for registration.

(3) The Commission may, within a period specified in the regulations, grant or reject the application submitted under subsection (2).

(4) The Commission shall issue a certificate of registration to the data controller or data processor who has fulfilled the prescribed requirements and registered under this section.

(5) Where the Commission rejects an application it shall inform the applicant in writing and give reasons for the decision.

Register of data controllers and data processors

15.-(1) The Commission shall establish and maintain a register of data controllers and data processors registered in accordance with this Act.

(2) The register shall contain such particulars as may be prescribed in the regulations.

(3) A data controller or data processor may, at any time, apply to the Commission to update or change any particulars in the register.

Duration of registration

16.-(1) The period of registration shall be five years from the date of issuance of certificate of registration.

(2) The application for renewal shall be submitted within the period of three months before expiry in the manner prescribed in the regulations.

Inspection of registered particulars

17. Subject to the procedures as may be prescribed in the regulations and upon payment of prescribed fees, the Commission may permit any person to inspect and extract any entry in the register.

Deregistration

18. The Commission may deregister any registration under this Act as may be prescribed in the regulations.

Offences relating to registration

19. Any person who contravenes the provisions of this Part or furnishes false or misleading information during registration or renewal, commits an offence and upon conviction shall be liable for a penalty specified under section 63.

Appeal relating to registration

20. Any person who is aggrieved by the decision of the Commission under this Part may appeal in writing to the Minister.

Registration of public institutions

21. Immediately after commencement of this Act, public institutions which collect and process personal data shall be deemed as registered with the Commission under this Act and shall be required to comply with the provisions of this Act.

PART IV
COLLECTION, USE, DISCLOSURE AND RETENTION OF PERSONAL DATA

Collection of

22.-(1) This Part shall be applicable to-

GN. NO. 395B (Contd)

personal data

(a) any collection and processing of personal data performed wholly or partly by manual or automated means;

(b) the processing of personal data carried out in the performance of activities of a controller domiciled in United Republic or in a territory where the laws of the United Republic apply by virtue of international public law; and

(c) the processing of personal data by a data controller or data processor who is not domiciled in the United Republic, if the processing of the personal data is in United Republic and such processing is not for the purposes of mere transit of personal data through Tanzania to another country.

(2) A data controller shall collect personal data if-

(a) the personal data is collected for a lawful purpose related to a function of the data controller; and

(b) the collection of the data is necessary or incidental or directly related to the lawful purpose.

(3) A data controller shall not collect personal data by unlawful means.

Source and notification of personal data

23.-(1) Subject to subsection (3), a data controller shall collect personal data directly from the data subject concerned.

(2) Before collecting data, a data controller shall ensure that the data subject is aware of-

(a) the purposes for which the personal data is collected;

(b) the fact that collection of the personal data is for authorised purposes; and

(c) any intended recipients of the personal data.

(3) A data controller is not obliged to comply with subsection (1) where-

(a) the personal data is publicly available;
(b) the data subject concerned authorises the collection of the personal data from a third party;
(c) compliance is not reasonably practicable in the circumstances of the particular case;
(d) non-compliance is necessary for compliance with other written laws; or
(e) compliance would prejudice the lawful purpose of the collection.

Accuracy of personal data

24. Subject to the purpose for which the personal data are intended to be used, a data controller who holds personal data shall not use that personal data without taking such steps as are, in the circumstances, reasonable to ensure that, the data is complete, accurate, relevant and not misleading.

Personal data to be used for intended purpose

25.-(1) Personal data collected under this Act shall be used for the intended purposes.

(2) Where a data controller holds personal data that was collected in connection with a particular purpose, he may use that personal data for other purposes if-

(a) the data subject authorises the use of the personal data for that other purpose;
(b) use of the personal data for that other purpose is authorised or required by law;
(c) the purpose for which the personal data is used is directly related to the purpose for which the personal data was collected;
(d) the personal data is used-
    (i) in a form in which the data subject is not identified; or
    (ii) for statistical or research purposes and shall not be published in a form that could reasonably be expected to identify the data subject;

(e) the data controller believes on reasonable grounds that use of the personal data for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the data subject or other person, or to public health or safety; or

(f) use of personal data for that other purpose is necessary for compliance with the laws.

Limitations on disclosure of personal data

26. Where data controller holds personal data, he shall not disclose the personal data to a person, other than the data subject except in the circumstances specified under section 25.

Security of personal data

27.-(1) A data controller and his representatives shall ensure that personal data is protected, by such security safeguards that is reasonable in the circumstances necessary for the personal data protection against negligent loss or unauthorised destruction, alteration, access or processing of the personal data.

(2) Security measures taken in accordance with subsection (1) shall ensure an appropriate level of security taking into account-

(a) the state of technological advancement and the cost of implementing the measures; and

(b) the nature of the personal data to be protected and the potential risks to the data subject.

(3) The data controller and data processor, as the case may be, shall appoint a data protection officer who shall ensure that the control and security measures are in place to protect the personal data collected or being processed.

(4) Implementation of activities of the data processor shall be governed by a contract which associates the data processor to the data controller to the effect that the data processor acts under instructions of the data controller and that the data processor is additionally, responsible for ensuring compliance of the

security standards as provided by this Act.

(5) The data controller shall notify the Commission, without any undue delay, of any security breach affecting personal data being processed by or on behalf of the data controller.

Retention and disposal of personal data

28.-(1) Where a data controller uses personal data for a specified purpose as specified under section 25, he shall retain that personal data for a period specified in the relevant laws or a period prescribed in the regulations in order to ensure that the data subject has a reasonable opportunity to access the personal data where need arises.

(2) Subject to subsection (1), the Minister may, by regulations prescribe the retention and disposal of personal data held by a data controller in accordance with the purpose of retention.

Correction of personal data

29.-(1) Where a document or file to which access has been given under this Act contains personal data and that data subject claims that the personal data-

(a) is incomplete, incorrect or misleading; or

(b) not relevant to the purpose for which the document is held,

the data controller may, subject to procedures as may be prescribed in the regulations and upon receiving and being satisfied with the application of the data subject, amend the personal data.

(2) The data controller shall, when making an amendment to personal data in a document under this section, ensure that he does not permanently delete the record of the text of the document as it existed prior to the amendment.

(3) Where a data controller is not satisfied with the reasons for an application under subsection (1), he may refuse to make any amendment to the personal data and inform the applicant of the reasons for refusal.

GN. NO. 395B (Contd)

Prohibition on processing of sensitive personal data

30.-(1) A person shall not process sensitive personal data without obtaining prior written consent of the data subject.

(2) The consent under subsection (1) may be withdrawn by the data subject at any time and without any explanation or charges.

(3) The Minister may, by regulations, determine circumstances in which the prohibition to process the personal data referred to in this section cannot be removed even with the data subject's consent.

(4) Where the data subject from whom consent is sought for the purpose of this Act, is a minor, a person of unsound mind or any other person unable to consent, such person's consent shall be sought from his parents, guardian, heirs, attorneys or any other person recognised by law to be acting on behalf of the person whose consent is to be sought.

(5) Subsection (1) shall not apply where-

(a) the processing is necessary for compliance with other written laws;

(b) the processing is necessary to protect the vital interests of the data subject or of another person, where the data subject is incapable of giving his consent or is not represented by his legal representative;

(c) the processing is necessary for the institution, trial or defence of legal claims;

(d) the processing relates to personal data which has apparently been made public by the data subject;

(e) the processing is necessary for the purposes of scientific research and the Commission has, by special guidelines, specified the circumstances under which such processing may be carried out; or

(f) the processing is necessary for the purposes of medical reasons in the interest of the data subject, and the sensitive personal data

concerned, is processed under the supervision of a health professional in accordance with the law governing such health care services.

PART V
TRANSBORDER DATA FLOW

Transfer of personal data to state with adequate personal data protection

31.-(1) The Commission may, subject to the provisions of this Act, prohibit the transfer of personal data to a place outside the country.

(2) Personal data shall be transferred to country that has a legal framework that provides for adequate data protection, if-

(a) the recipient establishes that the personal data is necessary for the performance of a task carried out in the public interest or pursuant to the lawful functions of a data controller; or

(b) the recipient establishes the necessity of having the data transferred and there is no reason to assume that the data subject's legitimate interests might be prejudiced by the transfer or the processing in the recipient country.

(3) The data controller shall, notwithstanding subsection (2), be required to make a provisional evaluation of the necessity for the transfer of the personal data.

(4) The recipient shall ensure that the necessity for the transfer of the personal data can be subsequently verified.

(5) The data controller shall ensure that the recipient shall process the personal data for the purposes for which it was transferred.

Transfer of personal data to state without adequate personal data

32.-(1) Personal data may be transferred to recipients states other than those referred to under section 31, if an adequate level of protection is ensured in the country of the recipient and the personal data is

protection

transferred solely to permit processing authorised to be undertaken by the controller.

(2) The adequacy of the level of protection afforded by the relevant third country shall be assessed in the light of-

(a) all the circumstances surrounding the relevant personal data transfer;

(b) nature of the personal data;

(c) the purpose and duration of the proposed processing;

(d) the recipient's country;

(e) the relevant laws in force in the third country; and

(f) the professional rules and security measures which are complied within that recipient's country.

(3) The Minister shall, after consultation with Commission and by regulations, specify categories of processing for which and the circumstances in which the transfer of personal data to countries outside the United Republic is not authorised.

(4) Notwithstanding the provisions of subsection (3), a transfer of personal data to a recipient in a country outside the country or to a country which does not have adequate level of protection may take place in one of the following cases-

(a) the data subject has consented to the proposed transfer;

(b) the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken in response to the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded or to be concluded between the data controller and a third party in the interest of the data subject;

(d) the transfer is necessary or legally required

on public interest grounds, or for the institution, trial or defence of legal claims;

(e) the transfer is necessary in order to protect the legitimate interests of the data subject; and

(f) the transfer is made in accordance with the law, and is intended to provide information to the public, and is open for consultation either by the public in general or by any person who can demonstrate a legitimate interest, to give his opinion in accordance with the conditions provided under the law.

(5) Without prejudice to the provisions of this Act, the Commission may authorise a transfer of personal data to a recipient country or any other country which does not have adequate level of protection in its laws, if the data controller satisfies the Commission that there is adequate safeguards with respect to the protection of personal data, fundamental rights and freedoms of the data subject and the exercise of the data subject's rights, and that such safeguards can be appropriated through adequate legal and security measures and contractual clauses in particular.

PART VI
RIGHTS OF DATA SUBJECTS

Right of access to personal data

33.-(1) Subject to the provisions of this Act, a data subject shall be entitled-

(a) to be informed by any data controller whether his personal data are being processed by or on behalf of that data controller;

(b) to be given by the data controller a description of-

(i) the personal data of which that individual is the data subject;

(ii) the purposes for which they are being processed; and

(iii) the recipients or classes of recipients to whom they are or may be disclosed;

(c) where the processing of personal data by automatic means for the purpose of evaluating matters relating to him has constituted or is likely to constitute the sole basis for any decision significantly affecting him, to be informed by the data controller of the logic involved in that decision making.

(2) Notwithstanding the provisions subsection (1), a data controller is not obliged to inform the data subject where the personal data-

(a) are not accurate;

(b) are involved in any investigation in accordance with the laws; or

(c) have been prohibited by court order.

Right to prevent processing likely to affect data subject

34.-(1) Subject to subsection (2), a data subject is entitled to require a data controller through procedures prescribed in the regulations, to suspend or not to begin, processing of any personal data in respect of which he is the data subject, if the processing of such personal data is likely to cause substantial damage to him or to another person.

(2) Subsection (1) shall not apply in the exceptions provided under this Act.

Right to prevent processing of personal data for direct marketing purposes

35.-(1) A data subject may, through the procedures prescribed in the regulations, require the data controller to stop processing his personal data for purposes of direct marketing.

(2) Subject to subsection (1), a data subject may enter into agreement with a data controller for purposes

of using or processing his personal data for pecuniary benefits.

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

Rights in relation to automated decision making

36.-(1) A data subject may, through the procedures prescribed in the regulations, require the data controller to ensure that any decision taken by or on behalf of the data controller which significantly affects data subject shall not base solely on the processing by automatic means.

(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 practicable, notify the data subject that the decision was taken on that basis; and

(b) the data subject may require the data controller to reconsider the decision.

(3) This section shall not apply if the decision is-

(a) necessary for entering into, or performance of, a contract between the data subject and a data controller;

(b) authorised by any written law; or

(c) based on the data subject's explicit consent.

Right to compensation

37.-(1) A data subject who suffers damage by reason of any contravention of any of the requirements of this Act by a data controller or data processor shall be entitled to compensation from the data controller or data processor for that damage.

(2) The data subject whose rights have been infringed by reason of any contravention of any of the requirements of this Act shall be entitled to compensation from the data controller or data processor, if-

(a) the complainant is the affected data subject or

a representative of a data subject where the data subject is a child or a person of unsound mind;

(b) the data subject's rights have been infringed by reason of the contravention; and

(c) the damage relates to the processing of personal data in contravention of the provisions of this Act.

(3) Where the Commission is satisfied on the application of a data subject-

(a) that he has suffered damage by reason of contravention of any of the requirements of this Act by a data controller or data processor in respect of any personal data, in circumstances entitling him to compensation under this section; and

(b) that there is a substantial risk of further contravention in respect of the personal data in such circumstances,

the Commission may order the rectification, blocking, erasure or destruction of any of the personal data.

(4) The Commission may, where it makes an order under subsection (3), and where it considers it reasonable, order the data controller or data processor to notify third parties to whom the personal data have been disclosed of the rectification, blocking, erasure or destruction.

(5) In determining whether it is reasonably practicable to require the notification in subsection (4), the Commission shall have regard, in particular, to the number of persons who need to be notified.

Rectification, blocking, erasure and destruction of personal data

38.-(1) Where the Commission is satisfied on the application of a data subject that his personal data is inaccurate, the Commission may order the data controller or data processor to rectify, block, erase, or destroy the personal data.

(2) Subsection (1) shall apply whether or not the

personal 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 personal data is not accurate record of the information, the Commission may direct the data controller or processor to correct the personal data as it considers appropriate.

(4) Where the personal data complained of has been rectified, blocked, updated, erased or destroyed under this section, the data controller or data processor shall be required to notify third parties to whom the personal data has been previously disclosed of the rectification, blocking, updating, erasure or destruction.

PART VII
INVESTIGATION OF COMPLAINTS

Complaints against violation of personal data protection principles

39.-(1) Any person who considers that a data controller or data processor has infringed personal data protection principles may file a complaint to the Commission.

(2) Where the Commission is satisfied that there are reasonable grounds to investigate a matter under this Act, the Commission may initiate an investigation in respect thereof.

(3) A complaint made under this section shall be investigated and concluded within ninety days from the date of receipt.

(4) The Commission may, taking into account the circumstances of the complaint, extend the time provided under subsection (3) up to a period not exceeding ninety days.

Notice of investigation

40. Before commencing an investigation of a complaint under this Act, the Commission shall, in a form prescribed in the regulations, notify the data controller or data processor concerned of the substance of the complaint and intention to carry out the

investigation.

Investigation confidentiality

41.-(1) Investigation of a complaint under this Act shall be conducted confidentially.

(2) The Director General or any person acting on his behalf who receives personal data relating to any investigation under this Act or any other written law shall satisfy any security requirements by taking any oath of secrecy required to be taken by persons undertaking tasks of the similar nature.

Powers of Commission in carrying out investigations

42.-(1) In the course of carrying out investigation of any complaint, the Commission shall have power to-

(a) summon a person before the Commission;

(b) receive and accept such evidence and other information, whether on oath or by affidavit or otherwise;

(c) enter any premises occupied by any data controller or data processor for satisfying security requirements of the premises;

(d) interrogate any person or take any device with personal data in any premises entered pursuant to paragraph (c); and

(e) examine or obtain copies of, or extracts from, books, documents or other records found in any premises entered pursuant to paragraph (c) containing any matter relevant to the investigation.

(2) In the course of an investigation of a complaint under this section, the complainant and the data controller or data processor concerned may be given an opportunity to make representations to the Commission.

(3) Notwithstanding any other written law, the Commission may examine any personal data recorded in any form held by a data controller or data processor and in doing so, no personal data shall be withheld from the Commission.

(4) Any document or articles produced pursuant to this section by data controller or data processor or any person shall be returned by the Commission within ten working days after a request is made to the Commission by the data controller or data processor or that person, but nothing in this subsection precludes the Commission from again requiring its production in accordance with this section.

Obstruction of Commission

43. A person who, in relation to the exercise of a power conferred by this Act-

(a) obstructs or impedes the Commission in the exercise of its powers;

(b) fails to provide assistance or information requested by the Commission;

(c) refuses to allow the Commission to enter any premises or to take any document or device with personal data; or

(d) gives to the Commission any information which is false or misleading;

commits an offence and shall be liable on conviction to a fine of not less than one hundred thousand shillings but not exceeding five million shillings or imprisonment to a term of not more than two years, or both.

Seeking assistance of any person or authority

44.-(1) For the purpose of gathering information or for any investigation under this Act, the Commission may cooperate with or use any person or other authority as it considers necessary to assist the Commission in the discharge of its functions.

(2) The person or another authority that will be involved or used by the Commission under subsection (1) shall have the same power as that of the Commission in exercising investigation powers under this Act.

Enforcement notice

45.-(1) Where the Commission is satisfied that a person has failed to comply with any provision of this Act, the Commission may serve an enforcement notice

on that person requiring such person to rectify the failure within such period as may be specified in the notice.

(2) An enforcement notice served under subsection (1) shall-

(a) specify the provision of this Act which has been contravened;

(b) specify the measures to be taken to remedy or eliminate the situation that leads to such contravention;

(c) specify a period that shall not be less than twenty-one days within which such measures shall be implemented; and

(d) state any right to appeal.

Notice of penalty

46.-(1) Where the Commission is satisfied that a person has failed or is failing to comply with the enforcement notice issued under section 45, the Commission may issue a penalty notice requiring the person to pay a fine to the Commission of an amount specified in the notice.

(2) In deciding whether to give a penalty notice to a person and determining the amount of the penalty, the Commission shall, so far as relevant, have regard to-

(a) the nature, gravity and duration of the failure;

(b) the intentional or negligent character of the failure;

(c) any action taken by the data controller or data processor to mitigate the damage suffered by data subjects including technical and organisational measures;

(d) any relevant previous failures by the data controller or data processor;

(e) the degree of co-operation with the Commission, in order to remedy the failure and mitigate the possible adverse effects of the failure;

(f) the categories of personal data affected by the failure;

(g) the manner in which the failure became known to the Commission, including whether the data controller or data processor notified the Commission of the failure;
(h) the extent to which the data controller or data processor has complied with previous enforcement notices or penalty notices;
(i) adherence to codes of ethics or terms and conditions of registration;
(j) whether the penalty would be effective; and
(k) any other aggravating or mitigating factor applicable to the case, including financial benefits gained, or losses suffered, as a result of the failure, whether directly or indirectly.

Administrative fines

47. The maximum amount of the penalty that may be imposed by the Commission in a penalty notice in relation to contravention of provisions of this Act is one hundred million shillings.

Review of decision

48.-(1) The Commission may, upon application or on its own motion, review its decision or direction given in accordance with the provisions of this Part.

(2) After review of the decision under subsection (1), the Commission may reverse, alter or revoke its decision or direction previously issued.

Right of appeal

49. A person who is aggrieved with the administrative action taken by the Commission, including the directions given in the enforcement notice or penalty imposed in the penalty notice, may appeal to the High Court.

Payment of compensation

50.-(1) Subject to the provisions of section 37, the Commission may, in addition to any penalty given under this Act, order a data controller or data processor who causes damages to the data subject following contraventions of any provisions of this Act to pay

compensation to the data subject.

(2) Subject to subsection (1)-

(a) a data controller involved in processing of personal data shall be liable for damage caused by the processing; and

(b) a data processor involved in processing of personal data shall be liable for damage caused by the processing if the processor-

(i) has not complied with an obligation under the Act specifically directed to data processors; or

(ii) has acted contrary to the data controller's lawful instructions.

(3) A data controller or data processor shall not be liable in the manner specified in subsection (2) if the data controller or data processor proves that he is not in any way responsible for the event caused the damage.

(4) In this section, "damage" includes financial loss and damage not involving financial loss.

PART VIII
FINANCIAL PROVISIONS

Sources of funds of Commission

51. The funds of the Commission shall consist of-

(a) such sums of moneys as may be appropriated by the Parliament;

(b) money accruing from services, consultancy or other payments;

(c) money received from donations, gifts or subsidies;

(d) loans; and

(e) such other income as derived from performance of functions under this Act.

Financial management

52. The funds of the Commission shall be managed and administered by the Board in accordance with financial laws and shall be utilised to defray

expenses in connection with performance of functions of the Commission under this Act.

Estimates of income and expenditure and financial control

53.-(1) The Director General shall, not less than three months before the end of each financial year, prepare and submit to the Board for approval the budget that includes the estimates of income and expenditure for the next financial year.

(2) Subject to the provision of subsection (1), the Commission shall submit a copy of the budget to the Minister for approval.

(3) The Minister may require the Commission to revise the budget if in his opinion the budget does not represent a fair and reasonable projection of income and expenditure.

Expenditure of funds

54. An expenditure shall not be incurred from the funds of Commission unless that expenditure is part of the expenditure approved by the Board under section 53(1) in respect of the financial year to which the expenditure relates.

Supplementary budget

55.-(1) The Board may, at any time before the end of the current financial year, prepare and submit to the Minister for approval any estimates supplementary to the estimates of the current year.

(2) Without prejudice to subsection (1), the Director General may, where exigencies occur in relation to the performance of the functions of the Commission, incur expenditure not approved by the Board in which case the Director General shall, within three months following such expenditure, seek approval of the Board.

Accounts and audit

56.-(1) The Commission shall keep books of account and maintain proper records of its operations in accordance with accounting standards.

(2) The Commission shall, within six months after the end of each financial year, prepares a report on

the performance of its functions during that financial year, and one copy of such report together with a copy of the audited accounts shall be submitted to the Minister.

(3) The accounts of the Commission shall be audited by the Controller and Auditor General or such other person registered as an auditor under the Auditors and Accountants (Registration) Act, appointed by the Controller and Auditor General for that purpose.

Cap. 286

Annual reports and performance agreements

57.-(1) The Director General shall, within two months after he has received audited accounts and auditor's report on those accounts, submit to the Minister an annual report in respect of that year containing-

(a) a copy of the audited accounts of the Commission, together with the auditor's report on those accounts;

(b) a report on performance against key targets and any other related information;

(c) a report on operations of the Commission during that financial year; and

(d) such other report as the Minister may require.

(2) The Minister shall lay before the National Assembly a copy of the annual report of the Commission within two month's or at the next meeting of the National Assembly.

PART IX
MISCELLANEOUS PROVISIONS

Exceptions from application of provisions of this Act

58.-(1) Nothing under this section shall exempt the data controller or the data processor from the responsibility of complying with the principles of the law in collection and processing of personal data and taking necessary measures to ensure protection and security of the personal data.

(2) Without prejudice to subsection (1), processing of personal data may be exempted from the provisions of this Act if such processing is held-

GN. NO. 395B (Contd)

(a) by the data subject for his personal use;
(b) in accordance with any law or court order;
(c) for purpose of safeguarding national safety and security and public interest;
(d) for the purpose of prevent or detect crimes;
(e) for the purpose of detect or prevent tax evasion;
(f) for the purpose of investigation of misappropriation of public funds;
(g) for purposes of vetting for appointment to any public service position.

(3) The Minister may prescribe other instances in which the provisions of this Act may be exempted and other provisions regarding implementation of this section.

Preservation order

59.-(1) The Commission may apply to a court for a preservation order for the expeditious preservation of any personal data including traffic personal data, where there is reasonable ground to believe that the personal data is vulnerable to loss or modification.

(2) Where the court is satisfied under subsection (1), that an order may be made under this subsection, it shall issue a preservation order specifying a period which shall not be more than ninety days during which the order shall remain in force.

(3) The court may, on application by the Commission, extend the period specified in subsection (2) for such time as the court thinks fit.

Offences of unlawful disclosure of personal data

60.-(1) A data controller who, without lawful excuse, discloses personal data in any manner that is incompatible with the purpose for which such personal data has been collected commits an offence.

(2) A data processor who, without lawful excuse, discloses personal data processed by the data processor

without the prior authority of the data controller commits an offence.

(3) Subject to subsection (4), a person who-

(a) obtains personal data, or obtains any information constituting personal data, without prior authority of the data controller or data processor by whom the personal data is kept; or

(b) discloses personal data to third party,

commits an offence.

(4) A person who offers for sale personal data of another person obtained in breach of subsection (1) commits an offence.

(5) For the purposes of subsection (4), an advertisement indicating that personal data is or may be for sale, constitutes an offer for sale of the personal data.

(6) A person who commits an offence under this section shall, upon conviction, be liable to-

(a) in the case of an individual, a fine of not less than one hundred thousand shillings but not exceeding twenty million shillings or to imprisonment for a term not exceeding ten years or both; and

(b) in the case of a company or corporation, a fine of not less than one million shillings but not exceeding five billion shillings.

Offences of unlawful destruction, deletion, concealment or alteration of personal data

61. A person who unlawfully destroys, deletes, misleads, conceals or alters personal data commits an offence and shall, upon conviction, be liable to a fine of not less than one hundred thousand shillings but not exceeding ten million shillings or to imprisonment for a term not exceeding five years or both.

Offences by company or corporation

62. Where an offence under this Act is committed by a company or corporation, the company or corporation and every officer of the company or corporation who knowingly and willfully authorises or

permits the contravention shall be liable for the offence.

General penalty

63.-(1) Any person who contravenes a provision under this Act commits an offence and where no penalty is specifically provided, shall, upon conviction, be liable to a fine of not less than one hundred thousand shillings but not exceeding five million shillings or imprisonment for a term not exceeding five years or to both.

(2) After conviction of a person for any offence under this Act, the court may order for forfeiture of the devices containing the personal data connected with the commission of an offence.

Regulations

64.-(1) The Minister may make regulations for giving effect to the provisions of this Act.

(2) Notwithstanding the generality of subsection (1), regulations made under this section may prescribe-

(a) instances which may be exempted from the provisions of this Act;
(b) registration procedures under this Act;
(c) functions of the data protection officer in relation to personal data protection;
(d) functions of the data controller's representative when collecting and processing personal data on behalf of the data controller;
(e) procedures of enforcing rights under this Act;
(f) procedures for submission of complaints under this Act;
(g) conditions for processing sensitive personal data;
(h) appropriate standards relating to security of information to be met by data controllers;
(i) various fees to be imposed in respect of implementation of the provisions of this Act;
(j) procedures for retention and disposal of personal data held by data controllers;

GN. NO. 395B (Contd)

(k) categories of processing and cases in which transborder data flow may not be allowed;

(l) anything which is necessary or proper for the better carrying out of the provisions of this Act.

Code of ethics for personal data protection

65.-(1) Every data controller shall draw and put in place a code of ethics or policy for personal data protection which shall prescribe for ethics and conduct to be complied with during collection or processing of personal data.

(2) Such codes or policies shall be submitted to the Commission for consideration and approval.

(3) In considering the codes of ethics or policies, the Commission shall ascertain, among other things, whether the drafts submitted to it have complied with the provisions of this Act and the relevant sector and where it considers necessary, seek the views of data subjects or their representatives and consult with the data controller concerned for the purposes of undertaking necessary amendments prior to the approval.

GN. NO. 395B (Contd)

SCHEDULE

(Made under section 8(6))

PROCEEDINGS OF THE BOARD

Tenure of appointment members

1.-(1) The tenure of members of the Board shall be as follows:

(a) a Chairman and Vice-Chairman - four years; and

(b) other members - three years.

(2) Each member shall be eligible for reappointment for one further term and thereafter shall not be eligible for re-appointment.

(3) Any member may at any time resign by giving notice in writing to the appointing authority and from the date specified in the notice or if no date is so specified, from the date of receipt of the notice by the appointing authority, he shall cease to be a member.

Cessation of members

2. A member of the Board may at any time cease from his office on the following reasons:

(a) inability to perform the functions of his office arising from infirmity of body or mind;

(b) misbehaviour or misconduct in a manner which bring or is likely to bring the Board into disrepute;

(c) absence from three consecutive meetings of the Board without notification;

(d) resigning; and

(e) death.

Absence from meetings of Board

3.-(1) Where any member absents himself from three consecutive meetings of the Board without notification, the Board shall advise the appointing authority of the fact and the appointing authority may terminate the appointment of the member and appoint another member in his place.

(2) Where any member is by reason of illness, infirmity or absence from the United Republic unable to attend any meeting of the Board, the Minister may appoint a temporary member in his place and any such temporary member shall cease to hold office on the resumption of office of the substantive member.

Proceeding not to be invalid by reason of irregularity

4. The proceedings of the Board shall not be invalid by reason only of any defect in the appointment of any member or of the fact that any member was at the time disqualified or disentitled as such.

GN. NO. 395B (Contd)

Meetings of Board

5.-(1) The Board shall meet in quarterly basis at such times and places as it deems necessary for the transaction of its business.

(2) The Chairman or, in his absence, the Vice-Chairman, may, convene a special or extraordinary meeting of the Board.

(3) An ordinary meeting of the Board shall be convened by the Chairman and the notice specifying the place, date and time of the meeting shall be sent to each member not less than ten days before the date of the meeting and where the Chairman is unable to act by reason of illness or other cause or is absent from the United Republic, the Vice-Chairman may convene the meeting.

(4) The Board may act notwithstanding any vacancy in its membership.

Conflict of interest

6.-(1) Where at any time a member of the Board has a conflict of interest in relation to-

(a) any matter before the Board for consideration or determination;

(b) any matter the Board could reasonably expect might come before it for consideration or determination,

the member shall immediately disclose the conflict of interest to the other members of the Board and refrain from taking part, or taking any further part, in the consideration or determination of the matter.

(2) Where the Board becomes aware that a member has a conflict of interest in relation to any matter which is before the Board, shall direct the member to refrain from taking part, or taking any further part, in the consideration or determination of the matter.

(3) A member of the Board shall be considered to have breached the provision of subparagraph (1) if-

(a) he fails without reasonable cause to make declarations of his interests as required; or

(b) he knowingly makes a declaration false or misleading in material particulars thereby affecting the decision,

that person commits an offence and shall be required to resign from office.

Invitation of expert

7. The Board may invite any person who is not a member to participate in the deliberations of the Board and provide expertise as the Board may require, but such person shall not be entitled to vote.

Quorum

8. The quorum at any meeting of the Board shall be more than half of the members in the Board.

Minutes of meetings

9. Minutes of each meeting of the Board shall be kept and shall be confirmed by the Board at its next meeting.

GN. NO. 395B (Contd)

Decision of Board

10. Decision of the Board shall be decided by majority of the vote of the members present and in the event of the equality of the vote the Chairman shall have a casting vote.

Board to regulate its own proceedings

11. Subject to the provisions of this Act, the Board shall regulate its own proceedings in relation to its meetings and discharge of its duties.

Remuneration of members

12. The members of the Board shall be paid such fees and allowances as may be determined by the relevant authority.