GOVERNMENT NOTICE No. 449C published on 4/7/2023

THE UNITED REPUBLIC OF TANZANIA

THE PERSONAL DATA PROTECTION ACT

(CHAPTER 44)

REGULATIONS

THE PERSONAL DATA PROTECTION (PERSONAL DATA COLLECTION AND PROCESSING) REGULATIONS, 2023

[SUBSIDIARY LEGISLATION]

This version of the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023 has been translated into English Language, and is published under section 84(4) of the Interpretation of Laws Act, Chapter 1.

THE PERSONAL DATA PROTECTION ACT,
(CAP. 44)

REGULATIONS

(Made under section 64)

THE PERSONAL DATA PROTECTION (PERSONAL DATA COLLECTION AND PROCESSING) REGULATIONS, 2023

ARRANGEMENT OF REGULATIONS

Regulations *Title*

PART III
PROCEDURES OF ENFORCING RIGHTS OF DATA SUBJECTS

PART IV
PROCEDURE FOR TRANSFER OF PERSONAL DATA OUTSIDE THE COUNTRY

PART V
OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS AND SECURITY STANDARDS DURING CONTROLLING AND PROCESSING OF PERSONAL DATA

PART VI
GENERAL PROVISIONS

SCHEDULES

THE PERSONAL DATA PROTECTION ACT,
(CAP. 44)

REGULATIONS

(Made under section 64)

THE PERSONAL DATA PROTECTION (PERSONAL DATA COLLECTION AND PROCESSING) REGULATIONS, 2023

PART I
PRELIMINARY PROVISIONS

Citation

1. These Regulations may be cited as the Personal Data Protection (Personal Data Collection and Processing) Regulations, 2023.

Application

2. These Regulations shall apply to Mainland Tanzania as well as Tanzania Zanzibar save that, in Tanzania Zanzibar, these Regulations shall not apply to non-union matters.

Interpretation

3. In these Regulations, unless the context otherwise requires-

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

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

"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 a natural person, legal person or public body

designated as such by that law and it includes his representative;

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

"personal data" has the meaning ascribed to it by the Act;

"sensitive personal data" has the meaning ascribed to it by the Act;

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

Cap. 44 "Act" means the Personal Data Protection Act;

and

"Minister" means the Minister responsible for communication.

PART II
PROCEDURE FOR REGISTRATION OF DATA CONTROLLERS AND DATA PROCESSORS

Application for registration

4.-(1) A person shall not collect or process personal data without being registered with the Commission as a data controller or data processor.

(2) A person who intends to collect or process personal data shall submit an application for registration to the Commission using Form No. 1 specified in the First Schedule and pay the fees specified in the Second Schedule of these Regulations.

(3) Subject to subregulation (2), applications for registration shall be accompanied by the following documents:

(a) in the case of a natural person, an identity document;

(b) in the case of a legal person, a certificate of incorporation or registration; and

(c) any other information as the Commission may determine.

Verification of applications for registration

5.-(1) The Commission shall, after receiving the application for registration under regulation 4, verify the application within seven days from the date of receiving

the application to satisfy itself on the validity and completeness of the information in the application.

(2) Subject to the provisions of subregulation (1), the Commission may, after verifying the application for registration, accept the application and register the data controller or data processor that has met the registration requirements or reject the application.

(3) The Commission shall, after accepting the application under subregulation (2), issue a registration certificate to the registered data controller or data processor in Form No. 2 set out in the First Schedule to these Regulations.

(4) Where the Commission after verification determines that there is insufficient or deficient information in the submitted application, it shall inform the applicant in writing of the areas of rectification to the information and return it for reverification.

Rejection of application for registration

6. Where the Commission reject the application for registration, it shall, within fourteen days from the date of the decision, inform the applicant in writing the reasons for rejection.

Registration period

7. The registration shall be valid for five years from the date of issuance of the registration certificate.

Renewal of registration certificate

8.-(1) The data controller or data processor may renew the registration certificate by submitting an application for renewal to the Commission within a period of three months before the date of expiry of the registration period.

(2) The applications for renewal of registration shall be submitted in Form No. 3 set out in the First Schedule and accompanied by the fees set out in the Second Schedule to these Regulations.

(3) Where the data controller or data processor has failed to submit an application to renew the registration certificate within the time specified in subregulation (1), he shall be required to apply for new registration.

Register

9.-(1) The Commission shall keep and maintain a register of registered data controllers and data processors.

(2) The register shall include the following information of thedata controllers and data processors:

(a) the name of the data controller or data processor;
(b) the address of the place of work;
(c) the type of personal data to be collected and processed;
(d) information of the data protection officer; and
(e) any other information as the Commission may direct.

Updating or rectification of information

10.-(1) A data controller or data processor shall, within fourteen days after the occurrence of any change of information entered in the register, notify the Commission in writing of such change.

(2) The Commission may, after receiving information in accordance with subregulation (1), update or rectify such changes as it deems necessary.

Searching or extraction of information

11.-(1) The Commission may allow any person to search or extracting any information entered in the register.

(2) Subject to subregulation (1), any person who needs to search or extract any information shall submit a written application to the Commission accompanied by fees as specified by the Commission.

Cancellation of registration

12. The Commission may cancel the registration after satisfying itself that the data processor or data controller-

(a) has given false or misleading information in relation to the provisions of registration;
(b) has violated the terms and conditions of registration provided under the Act;
(c) has repeated the commission of offence; or
(d) has refused to pay the fine imposed in accordance with the Act or these Regulations

within the time given.

Procedures for cancellation of registration

13.-(1) The Commission shall, before canceling the registration in accordance with regulation 12, issue a written notice within fourteen days to the data controller or data processor whose registration is canceled instructing him to give reasons why the registration should not be canceled.

(2) Subject to subregulation (1), the data controller or data processor shall, after receiving the notice, be required to give reasons within seven days as to why his registration should not be cancelled.

(3) The Commission may cancel the registration certificate upon being satisfied that the data controller or processor served notice under subregulation (1) has failed to give satisfactory reasons why his registration should not be cancelled.

(4) A data controller or data processor to whom the registration certificate has been cancelled shall be removed from the register and shall be required to surrender the registration certificate issued to him by the Commission and apply for re-registration pursuant to the provisions of these Regulations.

Appeal

14. A data controller or data processor who is aggrieved by the decision of the Commission may submit an appeal in writing to the Minister within seven days from the date of the decision of the Commission and the decision of the Minister shall be final.

PART III
PROCEDURES OF ENFORCING RIGHTS OF DATA SUBJECTS

Prevention of collection or processing of personal data

15.-(1) The data subject may apply to the data controller or data processor to suspend or not to begin the collection or processing of any personal data concerning him if the collection or processing is likely to cause substantial damage to him or to another person.

(2) The application to prevent the processing of personal data under subregulation (1) shall be submitted to

the data controller or data processor in Form No. 4 set out in the First Schedule and a copy shall be submitted to the Commission.

(3) The data controller or data processor shall, within seventy-two hours after receiving the application under subregulation (2) and without charging any fee-

(a) acknowledge receipt of the application and temporarily suspend the processing of personal data;

(b) indicate on the system that the processing of relevant personal data is restricted; and

(c) in case there is a third party to whom the personal data have been disclosed in any other way, notify such party that the personal data is restricted and require him to suspend processing them or remove them from his system.

(4) Subject to the provisions of subregulation (3), the data controller or data processor may execute the application to prevent processing by-

(a) temporarily remove personal data from the system and transfer them to another system;

(b) prevent the personal data from being obtained by third parties; and

(c) temporarily remove the prevented personal data of the data subject from the website or other public networks under its management.

(5) After temporarily suspending the processing of personal data under subregulation (3), the data controller or data processor shall, within a period of seven days from the date of temporary suspension of processing, consider the application to prevent processing and may accept or reject the application if he is of the opinion that the application is unreasonable.

(6) Where the data controller or data processor accepts the application to prevent processing, he shall suspend the processing and remove the personal data from the system and if there is a third party to whom the personal data was disclosed, he shall ask such party to stop using the personal data and remove them from his system.

(7) Where the data controller or data processor rejects the application under subregulation (5), he shall notify the applicant in writing and explain the reasons for the rejection.

(8) Where the data subject is aggrieved by the decision of the data controller or data processor of rejecting the application under subregulation (5), he may, within fourteen days from the date of receiving the notification of rejection of the application under subregulation (7), submit a complaint to the Commission in accordance with the regulations relating to settlement of complaints made under the Act.

(9) The data controller or data processor may, after expiry of the period for filing a complaint under subregulation (8) and in the event that no complaint has been submitted by the data subject, continue with the processing of personal data in accordance with the provisions of the Act.

Procedure for rectification of personal data

16.-(1) The data subject may apply to the data controller or data processor to rectify the personal data which are not correct, changed, outdated, incomplete or misleading by using Form No. 5 set out in the First Schedule to these Regulations and a copy shall be submitted to the Commission.

(2) The application to rectify personal data may be accompanied by necessary documents which may be used to rectify the relevant personal data as may be required by the data controller or data processor.

(3) The data controller or data processor may, within a period of fourteen days after receiving the application under subregulation (1), accept and rectify the personal data or reject the application for rectification of personal data.

(4) Where the data controller or data processor rejects the application to rectify the personal data submitted under subregulation (1), he shall notify the data subject in writing and give reasons for rejection.

Procedure for

17.-(1) The data subject may apply to the data

erasure or destruction of personal data

controller or data processor to erase or destroy the personal data held by the data controller or data processor where-

(a) such personal data are no longer required for the intended purpose;
(b) the data subject has withdrawn the consent that gives the data controller or data processor the right to retain the personal data;
(c) the data subject is no longer interested to continue with the processing;
(d) the processing of personal data is for commercial purposes and the data subject is unwilling for his personal data to be used commercially;
(e) the processing of personal data has violated the law;
(f) erasure or destruction of personal data is necessary according to law.

(2) Subject to the provisions of subregulation (1), the data subject may submit the application for erasure or destruction of his personal data to the data controller or data processor in Form No. 6 set out in the First Schedule to these Regulations and a copy shall be submitted to the Commission.

(3) The data controller or data processor shall, within a period of fourteen days, consider the application for erasure or destruction of personal data under subregulation (2) and may, subject to the provisions of subregulation (4), accept or reject the application.

(4) The right to erase or destroy the personal data shall not be exercised if the processing is necessary for one of the following reasons:

(a) to exercise the right to freedom of expression and information;
(b) to fulfill legal obligations; or
(c) for the implementation of duties carried out in the public interest or in the Government's jurisdiction.

(5) Where the data controller or data processor rejects the application to erase or destroy personal data

submitted under subregulation (2), he shall notify the data subject in writing and give the reasons for rejection.

Enforcement of rights on behalf of data subject

18.-(1) Where a person has been authorised by the data subject for the purpose of exercising rights on behalf of the data subject under the Act, the data controller or data processor shall handle the relevant issue in consideration of the best interests of the data subject.

(2) Where the data subject is a child, the data controller or data processor shall ensure that-

(a) the person exercising that right is properly identified;

(b) the child's personal data relating to commercial advertisements shall be collected and processed in accordance with the provisions of the Act and these Regulations; and

(c) the parent or guardian is informed of the risks of processing and protection in place.

(3) Where the data controller or data processor is uncertain on the existence of a relationship between an authorised person and a data subject, the data controller or data processor may withhold the application for the enforcement of rights on behalf of the data subject until proof of that relationship is presented and duly satisfied.

Rights in relation to automated decision making

19.-(1) The data controller or data processor shall, where a decision which significantly affects the data subject is based solely on the processing by automatic means, notify the data subject in writing in relation to the relevant processing.

(2) Notification to be provided under subregulation (1) shall state-

(a) basic information about the relevant processing and intended purpose;

(b) specific requirements for the existence of transparency and uniformity during processing;

(c) the procedure to be used to store the personal data;

(d) any effects likely to arise during processing and how they will be handled; and

(e) the right of the data subject to object the use of his personal data in commercial advertisements.

(3) Notwithstanding the provisions of this regulation the data subject shall have the right to reject the use of his personal data in the decision made by automatic means.

PART IV
PROCEDURE FOR TRANSFER OF PERSONAL DATA OUTSIDE THE COUNTRY

Application procedure for permission to transfer personal data out of country

20.-(1) A data controller or data processor who intends to transfer personal data outside the country, shall submit an application for permit to the Commission using Form No. 7 set out in the First Schedule to these Regulations.

(2) Applications for permit to transfer personal data under subregulation (1) shall include-

(a) particulars of the applicant;
(b) particulars of the recipient;
(c) particulars of the data subject;
(d) the type of personal data to be transferred;
(e) the purpose and necessity of transferring personal data;
(f) details of the security of personal data in the country of the recipient;
(g) consent of the data subject;
(h) date and time of sending personal data; and
(i) any other information as may be required by the Commission.

(3) The applicant shall, at the time of submitting the application under subregulation (1), submit proof that-

(a) the country receiving the personal data has ratified an international agreement providing requirements for the protection of personal data;
(b) there is an agreement between the United Republic and the country receiving the personal data regarding the protection of personal data;

or

(c) there is a contractual agreement between the person requesting the personal data and the recipient of the personal data who is outside the country.

(4) The Commission shall consider the application submitted under subregulation (1) within a period of fourteen days after receiving the application in accordance with the provisions of the Act and these Regulations.

(5) The Commission may, after considering the application under subregulation (4), accept or reject such application.

(6) The Commission shall, if it accepts an application under subregulation (5), issue a permit to transfer personal data in Form No. 8 set out in the First Schedule to these Regulation.

(7) Where the Commission rejects the application under subregulation (5), it shall notify the applicant in writing and give the reasons for the rejection.

Reasons for Commission to reject applications to transfer personal data out of country

21. The Commission may reject applications for permit to transfer personal data outside the country for the following reasons:

(a) the transfer of personal data endangers national security;

(b) the Commission has satisfied that there is no adequate protection of personal data in the country of recipient;

(c) the transfer of personal data is restricted by other written laws;

(d) application for permit to the transfer of personal data does not meet the requirements of regulation 20;

(e) other reasonable grounds which the Commission may deem necessary for the public interest.

Conditions for permission

22. The permit issued by the Commission shall be subject to the following conditions:

(a) the personal data shall be transferred to the

recipient authorised in the permit;

(b) personal data transferred shall be processed for the intended purpose only;

(c) personal data shall not be disclosed or transferred to another recipient without the approval of the Commission; and

(d) the processing of personal data transferred outside the country shall not violate the laws of the country.

PART V
OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS AND SECURITY STANDARDS DURING COLLECTION AND PROCESSING OF PERSONAL DATA

Obligations of data controller and data processor

23. The data controller or data processor when collecting or processing personal data shall ensure that the personal data are-

(a) collected or processed lawfully, fairly and transparently;

(b) collected for a legitimate and specified purpose;

(c) adequate and necessary for purposes for which is processed;

(d) accurate and where necessary, are 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 permit identification of data subject for no longer than is necessary for the purpose for which the persona data is processed;

(f) processed in accordance with the rights of the 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;

(h) not transferred abroad contrary to the provisions of this Act; and
(i) not applied in the existing circumstances without taking steps to ensure such data are complete, accurate, consistent with the content and not misleading.

Protection of personal data by design or by default

24. The data controller or data processor shall, in the processing of personal data-
(a) establish the personal data protection mechanism; or
(b) design technical measures to safeguard and implement the principles of protection of personal data.

Principle of lawfulness

25. The data controller or data processor shall, in implementing the principle of lawfulness during the processing of personal data, consider the following important factors:
(a) the purpose of the processing is carried out in accordance with of the provisions of the Act;
(b) the processing is necessary for the intended purpose;
(c) the data subject is granted autonomous right to freedom to control his personal data;
(d) the data subject possesses an understanding of what he consented to and there is a simplified means to withdraw consent; and
(e) restriction of processing of personal data where the legal basis or legitimate interest ceases to apply.

Principle of specific purpose

26. The data controller or data processor shall, in implementing the principle of specific purpose of personal data during processing, consider the following important factors:
(a) specifying the purpose for each processing of personal data;
(b) determining the legitimate purpose of processing personal data before designing

organisational measures to protect the personal data collected;

(c) ensuring a new purpose is compatible with the original purpose for which the personal data was collected;

(d) to conduct regular reviews to ensure that the processing is necessary for the purpose of which the personal data was collected; and

(e) use technical measures, including hashing and cryptography to intended person, to reduce the possibility of recurrence of the purpose of processing personal data.

Principle of security of personal data

27. The data controller or data processor shall, in implementing the principle of security of personal data during processing, consider the following important factors:

(a) having an operative means of managing policies and procedures for information security;

(b) assessing the risks against the security of personal data and putting in place measures to counter identified risks;

(c) conducting processing that is robust to withstand changes, regulatory demands, incidents and cyber-attacks;

(d) to ensure that only authorised personnels have access to the personal data necessary for their processing tasks;

(e) to ensure that the transfer of personal data is secured against unauthorised access and changes;

(f) securing the personal data storage from unauthorised use, access and alterations;

(g) keeping backups and logs to the extent necessary for the security of personal data;

(h) using audit trails and events monitoring as a routine security controls;

(i) protecting sensitive personal data with adequate measures and, where possible, keep

separate from the rest of the personal data;

(j) having in place procedures to detect, handle, report, and learn from personal data breaches; and

(k) regularly reviewing and testing software to uncover vulnerabilities of the systems supporting processing.

Principle of proportionality and necessity of personal data

28. The data controller or data processor shall, in implementing the principle of proportionality and necessity of personal data during processing, consider the following important factors:

(a) avoiding the processing of personal data in bulk if it is possible to process for the relevant purpose;

(b) limiting the amount of personal data collected to what is necessary for the intended purpose;

(c) ability to demonstrate the relevance of personal data to the relevant processing;

(d) pseudonymising personal data as soon as the data is no longer necessary to have direct identifiable personal data and storing identification keys separately;

(e) anonymising or deleting personal data where the personal data is no longer necessary for the purpose;

(f) making the personal data flow efficient to avoid additional duplication or unauthorised access; and

(g) applying the available and suitable technologies for data avoidance and minimisation.

Principle of accuracy of personal data

29. The data controller or data processor shall, in implementing the principle of accuracy of personal data during processing, consider the following important factors:

(a) ensuring personal data sources are reliable in terms of personal data accuracy;

(b) having personal data particulars being accurate

as necessary for the specified purpose;

(c) verifying the accuracy of personal data with the data subject before and at different stages of processing depending on the nature of personal data, according to the changes that may occur;

(d) erasing or rectifying inaccurate personal data without delay;

(e) mitigating the effect of accumulating errors in the processing chain;

(f) giving the data subject an overview on the processing and easy access to the personal data for accuracy control and rectification if necessary;

(g) having personal data accurate at all stages of the processing and carrying out accuracy tests at critical stages;

(h) updating personal data as necessary for the purpose; and

(i) using the technological and design features to decrease inaccuracy.

Principle of storage limitation of personal data

30. The data controller or data processor shall, in implementing the principleof storage limitation of personal data during processing, consider the following important factors:

(a) having clear internal procedures for deletion and destruction of personal data;

(b) determining the nature and duration of storage of personal data that is necessary for the intended purpose;

(c) formulating internal retention statements of implementation;

(d) ensuring that there is no possibility of re-identification of anonymous personal data or recover deleted personal data and testing whether this is effective;

(e) having the ability to justify necessity of the personal data retention period for the intended purpose and disclose the reasons for the storage

period; and

(f) determining the nature of personal data and length of storage necessary for back-ups and logs.

Principle of rights of data subject

31. The data controller or data processor shall, in implementing the principle ofrights of the data subject during processing, consider the following important factors:

(a) granting the data subject autonomous right to freedom to control his personal data;
(b) enable the data subject to communicate and exercise his rights;
(c) to eliminate any discrimination against the data subject;
(d) guarding against the exploitation of the needs or vulnerabilities of data subject; and
(e) incorporating human intervention to minimise biases that automated decision-making processes may create.

Appointment and duties of data protection officer

32. Subject to the provisions of the Act, the data controller or data processor shall appoint a data protection officer who shall have the following duties:

(a) to ensure compliance with the Act and these Regulations in the processing of personal data carried out by the data controller or data processor;
(b) to provide information on violations of the provisions of the Act or these Regulations committed in the processing by the data controller or data processor and advise rectification measures;
(c) to prepare and submit quarterly reports on the compliance of the Act to the Commission;
(d) handling the applications or complaints made by the data subject, his representative or another person to the data controller or data processor in relation to the collection or processing of personal data; and

(e) to perform any other duty as may be directed by the data controller or data processor.

Data protection impact assessment

33.-(1) Where the data controller or data processor determines that the processing of personal data is likely to affect the rights and freedom of the data subject, he shall, before carrying out such processing, conduct an impact assessment on the processing of the relevant personal data.

(2) For the purposes of subregulation (1), the data protection impact assessment shall cover the following personal data processing:

(a) automated decision-making with significant legal effect that includes the use of profiling or algorithmic means or use of sensitive personal data as an element to determine access to services that results in significant legal effects;
(b) use of personal data on a large-scale for a purpose other than that for which the personal data was initially collected;
(c) processing of biometric or genetic data;
(d) where significant changes occur at any stage of processing that may result in higher risks to data subject;
(e) processing of sensitive personal data relating to children or vulnerable groups;
(f) combining, linking or cross-referencing separate datasets where the datasets are combined from different sources and where processing is carried out for different purposes;
(g) large-scale processing of personal data;
(h) a systematic monitoring of a publicly accessible area on a large-scale;
(i) innovative use or application of new technological or organisational measures; or
(j) where the processing prevents the data subject from exercising his rights.

(3) Where a personal data protection impact assessment is required under subregulation (1), the data controller or data processor shall conduct the assessment using Form No. 9 set out in the First Schedule to these

Regulations.

Directions of Commission in assessment results

34.-(1) Where the results of the assessment indicate the possibility of occurrence of impact on the processing, the data processor shall request for the instructions of the Commission attaching the assessment report.

(2) The Commission shall, within a period not exceeding seven days from receiving the request under subregulation (1), satisfy itself with the report submitted and may give instructions to the relevant data processor to stop processing the personal data or continue processing with conditions as it deems appropriate.

(3) Where the Commission, after expiry of a period of thirty days from the date of submission of the data protection impact assessment report, has failed to give instructions, the data processor may continue with the processing.

(4) The Commission shall conduct periodic audits to monitor compliance with the data protection impact assessment report and any recommendations or instructions that may have been given by the Commission and take necessary action.

PART VI
GENERAL PROVISIONS

Offences and penalties

35. A person who contravenes the provisions of these Regulations, commits an offence and on conviction shall be liable for penalty as stipulated in the Act.

Complaints

36. The data subject or any interested person who is aggrieved or affected by the processing or any decision relating to personal data made by the data controller or data processor contrary to the Act or these Regulations, may submit his complaints to the Commission in accordance with the procedures prescribed in the regulations relating to the settlement of complaints made under the Act.

FIRST SCHEDULE

FORMS

FORM NO. 1

(Made under regulation 4(2))

APPLICATION FORM FOR THE REGISTRATION OF DATA PROCESSOR AND DATA CONTROLLER

PART 1 – BASIC INFORMATION	
Specify if you are registered as: Data Controller ☐ Data Processor ☐	
Name:	
Physical address: Region: District: Ward/Shehia: Road/Street/Village: Building/House Number: Postal Address:	
Mobile phone number: Telephone number: E-mail: Country: Sector:	
Institution - Private/Public:	
For public institutions: (Describe the type of institution)	

PART 2 – PERSONAL DATA		
Provide details of the various aspects of the personal data to be processed and the purpose of processing		
CLASSES OF DATA SUBJECT (Employee, customer, student, supplier, partner, shareholder etc.)	DETAILS OF THE PERSONAL DATA TO BE PROCESSED (Name, address, Identification number, etc.)	THE PURPOSE OF PROCESSING (Payment of wages, invoices, recognition of subscriber, subscription, etc.)

PART 3 – SENSITIVE PERSONAL DATA
Applicable ( ) Not applicable ( )

If applicable, please fill out the details below, otherwise please continue with Part 4

Please select a group of categories of sensitive personal data to be processed	Specify the purpose of processing sensitive personal data:
Political ideology or political affiliation	
Racial or ethnic origin	
Religious or philosophies beliefs	
Child	
Marital status and family information	
Mental or physical health	
Gender	
Biometric data	

PART 4 – TRANSFER OF PERSONAL INFORMATION OUTSIDE THE COUNTRY

Applicable ( ) Not applicable ( )

If applicable, please fill out the details below, otherwise please continue with Part 5.

List the country(ies):

PART 5 - SECURITY MEASURES OF PERSONAL DATA

S/N.	Describe the impact of personal data (non-authorised use/release, theft, hacking etc.)	Safeguards, security measures and enforcement measures to protect personal data eg. access control, guest logbook, personal data confidentiality and personal data security, etc.)
1		
2		
3		

PART 6: NUMBER OF EMPLOYEES (MARK BY TICK (✓))

An institution with 1-49 employees	
An institution with 50-99 employees	
An institution with more than 99 employees	

PART 7: GROSS SALES FOR THE PREVIOUS YEAR (MARK BY TICK (✓))

An institution with a total turnover of less than Tsh. 100,000,000 per year	
An institution with a total turnover of between Tsh. 100,000,000-500,000,000 per year	
An institution with a total turnover of above Tsh. 500,000,000.00	

I certify that all the information I have provided is accurate and complete and I hereby apply to be registered as a Data Controller or Data Processor.

Signature: _____

Name: _____

Position: _____

Date:_____

FORM NO. 2

(Made under regulation 5(3))

REGISTRATION CERTIFICATE

Registration Number: .....

Registration Date: .....

It is hereby certified that the Data Controller/Data Processor with the name below is registered in accordance with section 14/21 of the Personal Data Protection Act, No.11 of 2022.

Name:.....

Address:.....

E-mail:.....

Fax: .....

The nature of work he does……....

.....
Director General

FORM NO. 3

APPLICATION FORM FOR RENEWAL OF REGISTRATION OF A DATA PROCESSOR AND DATA CONTROLLER

(Made under regulation 8(2))

Specify if you are registering as a:

Data Controller ……. Data Processor …….

Name: …….

Physical address: ……

Region: ……

District: ……

Ward/Shehia: ……...

Road/Street/Village: ……

Building/House Number: ……..

Postal Address: ……

Mobile phone number: ……..……..

Telephone number: ……..…

E-mail: ……..…

Country: …….

Sector: ……

Institution- Private/Public: ……

For public institutions: (Describe the type of institution) ……

PART 2: DIFFERENT PURPOSE

Specify if the renewal is for a different purpose other than the initial collection or processing

……

……

……

…….....….

FORM NO. 4

APPLICATION TO PREVENT COLLECTION OR PROCESSING OF PERSONAL DATA

(Made under regulation 15(2))

NOTE:
(i) Documentary evidence substantiating the suspension or not to begin may be required.
(ii) *If a space provided in this Form is not sufficient, submit the information as an appendix*

A. APPLICATION BASIS

Mark the appropriate box with a tick (✓):
SUSPENSION ☐ NOT TO BEGIN ☐

B. PARTICULARS OF DATA SUBJECT

Name: .....
Identification Number: .....
Phone number: .....
E-mail: .....
(State below if the data subject is a child or a person with disability)
Name: .....
Relationship with the Applicant: .....
Contact: .....

C. REASONS FOR THE APPLICATION

(Please provide detailed reasons for the application for suspension or not to begin the processing)

D. DECLARATION

I certify that the statements I made in this application are true

Date _____ Signature _____

FORM NO. 5

(Made under regulation 16(1))

APPLICATION FOR RECTIFICATION OF PERSONAL DATA

Note:

(i) Any documentary evidence in support of the application may be attached.

(ii) Where the space provided for in this Form is inadequate, submit information as an Annexure to this Form.

*(iii) All parts marked * are mandatory.*

A: PARTICULARS OF THE DATA SUBJECT

(This Part is for details of Data Subject)
Name*: ……
Identification Number*: .....
Phone number*: .....
E-mail:.....

(State below if the data subject is a child or a person with disability)
Name: .....
Relationship with the Applicant: .....
Contact: .....

Sign …….. Date …….

PROPOSED RECTIFICATION (S)

	Personal data currently to be rectified Name, physical address, mobile number, etc.	*The proposed rectification*	*Reason for the proposed rectification*
1.			
2.			
3.			

B: DECLARATION

I certify that I have read and understood the terms of this Form and confirm that the information given in this application is true.
(Please note that any attempt to gain access to personal data through misrepresentation may result in prosecution.)

Signature ……. Date ……..

FORM NO. 6

(Made under regulation 17(2))

APPLICATION FORM FOR ERASURE

Fill as appropriate

Note:

(i) Any documentary evidence in support of the application may be attached.
(ii) Where the space provided for in this Form is inadequate, submit information as an Annexure to this Form.
*(iii) All parts marked * are mandatory.*

i. PARTICULARS OF DATA SUBJECT

(This Part is for details of Data Subject)
Name*: ……
Identification Number*: .....
Phone number*: .....
E-mail:.....

(State below if the data subject is a child or a person with disability)
Name: .....
Relationship with the Applicant: .....
Contact: .....

ii. REASONS FOR ERASURE OF PERSONAL DATA

(Mark the appropriate box with a tick (✓))
Specify the reason(s) for which you want the personal data to be erased.

(a) The personal data is no longer necessary for the purposes for which was originally collected	
(b) You have withdrawn the consent that was the legal basis for the storage of personal data;	
(c) You are objecting to the processing of your personal data and there is no legal interest to proceed with the processing;	
(d) Your personal data has been unlawfully processed;	
(e) You are required to fulfil legal obligations.	

iii. DECLARATION

I confirm that I have read and understood the terms of this application form and certify that the information given in this application is true.
(Please note that any attempt to gain access to personal data through misrepresentation may result in prosecution.)

Signature: ..... Date: .....

FORM NO. 7

(Made under regulation 20(1))

APPLICATION FORM FOR PERMIT TO TRANSFER PERSONAL DATA OUTSIDE THE COUNTRY

I. PARTICULARS OF THE APPLICANT
Name.....
Identification Number …….

Data Controller /Data Processor……

Physical Address ……..……

Postal Address ……..……..

Phone Number: .....

Email Address: .....

II. PARTICULARS OF THE RECIPIENT
Name.....

Identification Number …….

Data Controller /Data Processor……

The Country of the Recipient ……..……..

Physical Address ……..……

Postal Address ……..……..

Phone Number: .....

Email Address: .....

III. PARTICULARS OF THE DATA SUBJECT
Name .....

Citizenship ……

Age ……..……

Gender ……..……

Identification Number …….

Phone Number: .....

Email Address: .....

(State below if the data subject is a child or a person with disability)

Name .....

Citizenship ……

Age ……..……

Gender ……..…..……

Identification Number …….

Relationship with the Applicant: .....
Contact: .....

I certify that the information provided in this application are true.

IV. THE CATEGORY OF THE PERSONAL DATA TO BE TRANSFERRED
……
……

V. THE PURPOSE AND NECESSITY OF TRANSFER THE PERSONAL DATA
……
……
……
……

VI. STATEMENT OF SECURITY OF PERSONAL DATA IN THE COUNTRY OF RECEIVER:

(Mark with a tick on the appropriate information)

i. The country you are requesting to transfer personal data has a Personal Data Protection Law;
ii. A country receiving personal data has ratified the International Convention making provisions in relation to the protection of personal data;
iii. There is an agreement between the United Republic and the country that receives data on the protection of personal data; or
iv. There is a contractual agreement between the data applicant and the person receiving the personal data who is outside the country.

VII. DATE AND TIME OF TRANSFER OF PERSONAL DATA: ……/……../……

VIII. ANY OTHER INFORMATION NEEDED BY THE COMMISSION ……
……
……

IX. CONSENT OF DATA SUBJECT:

I consent to my personal data being transferred outside the country as provided in this form.

SIGNATURE OF THE DATA SUBJECT DATE

…… ……/……..20……

SIGNATURE OF THE APPLICANT DATE

…… ……/……..20……

FORM NO. 8

(Made under regulation 20(6))

PERMIT NUMBER ….....

A PERMIT TO TRANSFER PERSONAL DATA
OUTSIDE THE COUNTRY

The Commission after considering the application submitted by the applicant and subject to the provisions of the Personal Data Protection Act and its Regulations has accepted the application of .....……, the Applicant (Data Controller/Data Processor), of transferring the personal data of ……...… *(Data Subject),* to ……...…., the Recipient of …….. *(Country),* on the ……. /……...20…… *(date)*

The Commission has therefore approved that the Data Controller/Data Processor mentioned in this Permit may transfer Personal Data out of the country as requested in accordance with sections 31 and 32 of the Personal Data Protection Act, No.11/2022.

GIVEN with the stamp of the COMMISSION this ……... day of ……..… 20……..

_____

DIRECTOR GENERAL OF THE COMMISSION

FORM NO. 9

DATA PROTECTION IMPACT ASSESSMENT (DPIA)
(Made under regulation 33(3))

Part 1: Details of processing operations

Name of Data Controller/ Data Processor: ..... Postal Address: ..... Email: ..... Telephone number: ..... Physical address: .....
1. Project/Activity Name
2. The need to conduct a data protection impact assessment. (Assessment, if there is a need for DPIA to explain if the project involves personal data that may cause significant impact, mention the impact where appropriate)
3. Brief description of the Project/Activity: *(Explain clearly what the project aims to achieve and what type of processing it involves)*
4. Personal Data *(The type of personal data being processed)*
5. Explain the Data Flow *Explain the collection, use and deletion of personal data, including; where you are getting the data from; the manner in which data is collected; where the data will be stored; the period for which the data will be stored; the number of people who will be affected by the relevant activity/Project.*
6. Explain how the data processing flow complies with the principles of protection of personal data:

Part 2: An assessment of the necessity and proportionality of the processing operations in relation to the purpose.

Assessment required and standards of assessment.

Explain consideration and balance, especially the measures taken	
The principles of lawful processing	
Means of obtaining the consent	
If the processing of personal data is necessary to achieve your purpose?	

Is there another way to achieve your purpose without processing personal data?	
Quality of personal data	
Adequacy of personal data	
Informing the data subject about processing activities	
Implementation of the rights of the data subject	
All parties involved in the processing and their specific roles	
Ensure existing procedures are complied with by all parties	
Security of personal data processing	
Security of personal data before crossing the borders of the country	

Part 3: Measures set to deal with risks and protection, security measures and procedures to ensure the protection of personal data and compliance with the Act.

Assessments of risks - Identifying personal data protection risks and assess how to address them

Identification of Risk and its Details	Impacts	Risk Owner	Current internal controls (provide details of how you currently managed the Risks) Current internal	Risk Assessment	Explain further steps you will take to reduce the impact/risk of the impact. Explain the owner of the risk at each step

Part 5: Conclusions and Results

DETAILS	TIPS/DIRECTIONS
Consultation with the Personal Data Protection Commission (where applicable)	
DPIA This will be placed under audit with:	

SECOND SCHEDULE

(Made under regulations 4(2) and 8(2))

FEE

Category	Particulars	Registration fee (Tsh) by the Data Controller /Data Processor) (To be paid once)	Renewal fee (Tsh) by the Data Controller /Data Processor) (To be paid after every 5 years)
Small-scale Data Controllers and Data Processors	Data Controllers and Data Processors with 1-49 employees and turnover of less than 100 million shillings per year.	100,000.00	50,000.00
Medium-scale Data Controllers and Data Processors	Data Controller or Data Processors with 50-99 employees and turnover of 100,000,000 to 500,000,000 per year.	200,000.00	150,000.00
Large-scale Data Controllers and Data Processors	Data Controllers or Data processors with 100 employees and a turnover of 500,000,000 shillings per year	1,000,000.00	500,000.00
Public institutions	Data Controller or Data Processors providing Government services (Regardless of the number of employees or income/turnover)	100,000.00 -500,000.00	50,000 - 300,000.00
Non-commercial and religious institutions	Data Controllers or Data Processors that provide charity or religious works (Regardless of income/turnover)	100,000.00	50,000.00