Job description and Specification

POST TITLE	**Data Protection Officer**
POST GRADE	**GMG/SEG 2**
POST NUMBER	**339689**
DIVISION	**Executive Office**
REPORTS TO	**Chief Executive Officer**
DIRECT REPORTS	**N/A**

This document is validated as an accurate and true description of the job when the agreement is signified below.

Approved by: ***Chief Executive Officer***

Signature: Date:

_____ _____

Received by:

I have received, read and fully understand the requirements of the job as outlined.

Signature: Date:

_____ _____

JOB PURPOSE

Under the general direction of the Chief Executive Officer, the Data Protection Officer has the responsibility to monitor compliance and data practices to ensure the Authority and its functions comply with the applicable legislative requirements under the Data Protection Act (2020) in the processing of the personal data of its staff, customers, providers or any other individuals.

The Data Protection Officer will serve as the primary contact for supervisory authorities and individuals whose data is processed by the Authority.

KEY OUTPUTS

- External regulations (Data Protection Act) and internal controls adhered to;
- Data Protection framework and strategy developed and implemented;
- Data protection impact assessments conducted;
- Breaches identified and notifications prepared;
- Reports prepared and submitted;
- Continuous monitoring conducted;
- Adherence/compliance with standards monitored;
- Governance and accountability mechanisms evaluated and recommendations made;
- Research and analysis conducted and findings documented;
- Continuous improvement strategies developed and implemented;
- Advice and recommendations provided;
- Sensitization sessions conducted.

KEY RESPONSIBILITY AREAS

Technical/Professional Responsibilities

- Implements strategies and a privacy governance framework to manage data used in compliance with the Data Protection Act;
- Develops and implement a privacy governance framework and strategies to manage data use;
- Collaborates with the Information Technology & Business Services Section in the maintenance of a data security incident management plan to ensure timely remediation of incidents including impact assessments, security breach response, complaints, claims or notifications and responding to subject access requests;
- Monitors to ensure that the Authority's ICT Systems and procedures comply with the relevant data privacy and protection law, regulation and policy;
- Evaluates existing policies and procedures to coordinate internal practices and to ensure compliance with regulations;

- Reviews the Authority's internal control mechanisms to ensure that they are aligned with standards outlined in the Data Protection Act;
- Reviews and document legal basis for processing personal data;
- Periodically revising the data protection plan in light of changes in laws, regulations and policies;
- Identifies compliance breaches as they arise and advise management on rules and controls;
- Provides legislative advice and guidance to the Executive as to gaps identified from the outcome of the Data Protection and Privacy Impact Assessment process;
- Serves as the primary point of contact for the Lead Supervisory Authority on all data protection matters;
- Consults with the Office of the Information Commissioner to resolve any doubt about how the provisions of the Act and its regulations are to be applied;
- Collaborates with Risk, Internal Audit, Legal and other key stakeholders to monitor, implement and analyze compliance programmes;
- Engages in the timely collection of data, analysis and reporting on key performance measures;
- Receives and responds to comments and queries from data subjects related to the processing of personal data;
- Establishes a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the organization's privacy policies and procedures;
- Provides guidance and assistance to data subjects in exercising their rights under the Act (Section 6-13) as it relates to: The right to Access, the right to prevent processing, The right in relation to automated decision making and the right to rectification;
- Provides advice/information to the Authority and its employees on their obligations under the Act and state data protection provisions;
- Manages and conducts ongoing reviews of the Authority's privacy governance framework;
- Conducts data protection impact assessments by applying data quality controls as prescribed in the Data Governance Framework to determine compliance with regulatory requirements;
- Shares current information on policies, procedures and legislation that the Authority's staff should be aware of so as to promote the quality culture;
- Develops and implements approved certification mechanisms to demonstrate compliance;
- Collaborates with senior managers in the review and understanding of corporate governance guidelines pertaining to data protection;
- Keeps abreast of amendments to policies, procedures and legislation and any pertinent developments within the dynamic environments;
- Monitors and evaluates Authority's efforts at corrective actions to ensure that findings and recommendations (weaknesses and or deficiencies) are effectively dealt with;
- Prepares reports and presentations on findings and analysis;

- Develops strategies and initiatives to ensure engagement with key internal and external stakeholders;
- Facilitates the training of staff on the components of the Act, Regulations and policies;

Other Responsibilities

- Any other related duties that may be assigned from time to time

KEY INTERFACES

Internal	***Purpose***
Chief Executive Officer	Receive directives & work assignments. Requests for information and dissemination of information pertinent mainly to ensuring ongoing compliance with policies, guidelines and the Act.
Divisional heads, managers and supervisors	Requests for information and dissemination of information pertinent mainly to ensuring ongoing compliance with policies, guidelines and the Act.
General Staff	Requests for information and dissemination of information pertinent mainly to ensuring ongoing compliance with policies, guidelines and the Act.

External	***Purpose***
Office of the Information Commissioner	Obtain and share information relating to the administration of the act.
Ministries/Departments/ Agencies of Government	Clarification on submissions and providing requested information
Auditors, Clients, Shareholders, Consultants etc.	Requests for information, responses, compiled and dispatched
Regional/International partners, regulators, technical compliance trainers.	Participation in any local, regional and international conferences, specialized training and knowledge sharing fora.

PERFROAMNCE STANDARDS

- Personal data processed in compliance with established ISO data protection standards;
- Data protection framework developed and implemented in accordance with established standards and guidelines;
- Monitoring and Evaluation framework developed and implemented in accordance with established guidelines;
- Technical reports, reviews and analyses completed within agreed timeframe;
- Quality, soundness and timeliness of advice, reviews and reports containing findings, assessment and recommendations;
- Breaches and infractions are detected and communicated to the Executive within the agreed timeframe;
- Sensitization sessions conducted in accordance with established guidelines and framework;
- Confidentiality, integrity and sensitivity are displayed in the execution of duties at all times.

REGUIRED COMPETENCIES

Core	Level	Technical/Functional	Level
Oral communication	3	Initiative	3
Written communication	3	Knowledge of modern business practices and office procedures	3
Planning and Organizing Skills	3	Understanding of research methods and techniques	3
Good Judgement and Decision Making Skills	3	Proficiency in the use of computer applications	4
Customer and Quality-focused skills	3	Knowledge and understanding of the Data Protection Act	4
Analytical and problem-solving skills	4	Experience in managing data incidences and breaches	4
Compliance	4	Knowledge of cybersecurity risks and information security standards	4
Integrity	4		
Adaptability	3		

MINIMUM REQUIRED EDUCATION AND EXPERIENCE (at least one from the list)

- Bachelors' degree in Law, Computer Science, Audit or equivalent qualification from recognized tertiary institution;
- Certification in Information Security, Data Protection and/or Privacy Certification such as CIPP,CIPT, ISEB, etc. (preferred);
- Exposure to legal training;
- Three (3) years related work experience.

SPECIAL CONDITIONS ASSOCIATED WITH TH JOB

- Pressured working conditions with numerous critical deadlines
- May be required to work abnormal working hours
- May be required to travel locally and overseas

AUTHORITY

The DPO has the authority to investigate and have immediate access to all personal data and data processing operations and to perform his/her duties independently.

Specifically, the Data Protection Officer must:

- handle queries or complaints on request by the Ministry, the controller, other persons, or on his/her initiative.
- ensure that any other tasks or duties assigned to the DPO do not result in a conflict of interest with his/her role as a DPO.
- Recommends appropriate standards;
- Recommends improvements in corporate governance framework;
- Recommends changes to regulatory framework;