SOUTHERN REGIONAL HEALTH AUTHORITY

Compassion | Accountability | Respect | Efficiency
3 Brumalia Road, Mandeville, Manchester, Jamaica WI
Tel: (876) 625-0612-3 / 962-9491 / 962-8232
Website: www.srha.gov.jm

The Southern Regional Health Authority (SRHA), a Statutory Body under the Ministry of Health & Wellness responsible for the management and operation of Public Health Services within the Parishes of Clarendon, Manchester and St. Elizabeth, invites applications from suitably qualified persons for the following position in the **REGIONAL OFFICE**:

DATA PROTECTION OFFICER (GMG/SEG 2 – Band 8) – VACANT
(salary range $4,266,270 – $5,737,658 per annum and any applicable allowances)

Job Purpose

The Data Protection Officer (DPO) is responsible for monitoring the Southern Regional Health Authority's (SRHA) data practices, ensuring that all functions carried out by the SRHA are in accordance with the provisions of the Data Protection Act (2020). Under the general direction of the Senior Director – Corporate Services, the DPO will be accountable for overseeing, monitoring internal compliance and providing guidance to the SRHA on data protection obligations. Additionally, the DPO will serve as a primary point of contact for supervisory authorities such as Office of the Information Commissioner (OIC) and individuals whose data is processed by the SRHA.

The DPO will provide specialist advice and support to the SRHA's senior management and will work closely with key internal stakeholders such as Legal, ICT, HRM & D, Audit, Operations and Procurement and manage relationships with key stakeholders.

Minimum Required Qualifications and Experience

The ideal candidate must possess:

- Undergraduate Degree in Information Security, Law, Computer Science, Information Technology, Data Privacy, or a related field

PLUS

- At least one (1) International Association of Privacy Professionals (IAPP Certifications):
  - Certified Information Privacy Professional (CIPP)
  - Certified Information Privacy Manager (CIPM)
  - Certified Information Privacy Technologist (CIPT)

OR

- At least one (1) ISACA certification in governance and risk management:
  - Certified in Risk and Information Systems Control (CRISC)
  - Certified in Governance of Enterprise IT (CGEIT
  - Certified Information Security Manager (CISM)

Relevant Experience

- At least 3-5 years' work experience in Privacy, Compliance, Information Security, Auditing, or a relevant field (Finance, Law, Business Administration, Information Technology)
- Sound knowledge of the Access to Information Act and anti-corruption laws.
- Experience in the following areas is an asset:
  - mapping/ understanding business processes and data handling or processing needs in a relevant/ related industry
  - Cybersecurity - dealing with real security incidents, risk assessments, countermeasures and data protection impact assessments.

Required Knowledge, Skills and Competencies

- Good oral and written communication
- Excellent analytical and problem-solving and decision-making skills
- Excellent interpersonal and customer service skills
- Excellent presentation, oral and written communication skills
- Excellent planning and organizing skills
- Ability to lead and work in team
- Good time management skills
- Ability to manage internal and external relationships
- Knowledge of Data Protection Laws & Practices

- Working knowledge of Auditing Techniques and Practices
- Risk Management Techniques and Strategies
- Knowledge of GOJ policies, programmes and the machinery of government
- Knowledge of Health Systems
- Knowledge of Legislation relating to the Health Service and the operations of the SRHA
- Project Management practices and principles
- Competency in the use of Microsoft Office Suite
- Good organizing skills
- Ability to maintain confidentiality
- High degree of integrity and diplomacy

Key Responsibilities

The duties and responsibilities include but are not limited to the following:

Technical/Professional

- Designing and implementing a comprehensive Data Privacy Governance Framework and strategies to effectively manage the use of personal data in accordance with the provisions of the Data Protection Act;
- Establishing and maintaining appropriate systems and internal control mechanisms that align with the prescribed standards of the Data Protection Act;
- Ensuring that the SRHA and its operational processes pertaining to data processing adhere to the established data protection standards and regulations;
- Implementing strategies to enhance operational processes and ensures processes comply with regulatory requirements and good practice;
- Designing and implementing Data Protection policies and procedures within the SRHA;
- Ensuring that breaches of the Data Protection standards or violations of the provisions outlined in the Data Protection Act are addressed promptly;
- Ensuring that any contravention of the data protection standards or any provisions of the Data Protection Act by the SRHA is dealt with in accordance with the provisions of the Data Protection Act;
- Notifying the SRHA of any contravention of the data protection standards or any provisions of the Data Protection Act;
- Reporting any contravention of the data protection standards or any provisions of the Data Protection Act to the OIC;
- Assisting data subjects in the exercise of their rights under the Data Protection Act, in relation to the SRHA;
- Assisting SRHA with the development of internal policies and procedures related to the processing of personal data.
- Making recommendations for the appropriate organizational and technical measures to ensure the security of personal data.
- Reviewing and updating the Data Protection Plan regularly to ensure it aligns with any changes in laws, regulations and policies;
- Ensuring the timely collection of data, analysis and reporting of data on key performance measures;
- Maintaining a robust system to address and respond to queries and complaints;
- Ensuring proper management and maintenance of personal data records, in compliance with data protection standards;
- Sensitizing and training staff on the components of relevant Acts, Regulations and Policies related to data;
- Informing data controllers and data subjects about their rights, obligations and responsibilities regarding data protection;
- Providing advice and recommendations to staff and the Regional Director regarding the interpretation and application of data protection rules;
- Collaborating with the Information and Communication Technology (ICT) Unit to ensure compliance with the Data Protection Act in the SRHA's ICT System;
- Collaborating with the Information and Communication Technology (ICT) Unit to manage data security incidents and ensures timely resolution of issues such as security breaches, complaints or subject access requests;
- Providing legislative advice and guidance to the Regional Director regarding any gaps identified from the outcome of the Data Protection and Privacy Impact Assessment;
- Liaising with the Office of the Information Commissioner (OIC) to address data protection matters and clarifies or resolves any doubts regarding the application of the act's provisions;
- Collaborating with the Enterprise Risk Management Unit, Internal Audit Division, Legal Services Division and other key stakeholders to monitor, implement and analyze compliance programmes;

Applications accompanied by resumes should be submitted no later than **Wednesday, December 24, 2025** to:

Director, Human Resource Management & Development
Southern Regional Health Authority
3 Brumalia Road
Mandeville

E-Mail: jobs@srha.gov.jm

PLEASE INDICATE THE NAME OF THE POSITION YOU ARE APPLYING FOR IN THE 'SUBJECT LINE' OF YOUR EMAIL*

****IMPORTANT NOTE: WE WILL ONLY ACCEPT APPLICATIONS BY EMAIL****

PLEASE INDICATE IN THE 'SUBJECT LINE' OF YOUR EMAIL THE NAME OF THE POSITION FOR WHICH YOU ARE APPLYING**

NB. ONLY SHORTLISTED APPLICANTS WILL BE ACKNOWLEDGED