



## Office of the Services Commissions

(Central Government)  
Ministry of Finance and the Public Service Building  
30 National Heroes Circle, Kingston 4  
Jamaica, West Indies  
Tel: 876-922-8600  
Fax: 876-924-9764  
Email: [communications@osc.gov.jm](mailto:communications@osc.gov.jm)  
Website: [www.osc.gov.jm](http://www.osc.gov.jm)

### **CIRCULAR No. 363** **OSC Ref. C. 6272<sup>18</sup>**

**13<sup>th</sup> September, 2024**

Permanent Secretaries, Heads of Department and Chief Executive Officers are asked to invite applications from suitably qualified officers in their Ministries/Departments/Agencies to fill the **vacant** post of **Data Protection Officer (GMG/SEG 3)** in the **Central Administration Branch, Office of the Prime Minister**, salary range \$5,198,035 - \$6,990,779 per annum.

#### **Job Purpose**

Under the general supervision of the Permanent Secretary through the Chief Technical Director, the Data Protection Officer (DPO) is responsible, in an independent manner, for:

- designing and overseeing the implementation of an effective data protection/data privacy programme in keeping with the Data Protection Act (DPA) and attendant regulations and other relevant legislation;
- monitoring the organisation's compliance with the DPA and attendant regulations, other relevant legislation, and the organisation's internal data protection/privacy policies and procedures;
- facilitating the conduct of risks assessments to, among other things, inform the preparation of Data Protection Impact Assessments (DPIA);
- informing and advising the organisation on its data protection/data privacy obligations pursuant to the DPA;
- building awareness of data privacy/data protection by all staff through training and sensitization initiatives.

The DPO serves as the primary point of contact within the organisation for members of staff, the Office of the Information Commissioner (OIC), data subjects and any relevant entity on issues related to data protection/data privacy.

#### **Key Responsibilities**

##### ***Management/Administrative:***

- Provides overall management for the development and implementation of an effective data protection/data privacy programme, in keeping with the DPA and attendant regulations and other relevant legislation;
- Assesses the organisation's business processes and workflows;
- Participates in the Organisation's strategic planning process;
- Prepares strategic and operational plans and budget, ensuring the work is performed according to plan and agreed targets;
- Participates, as a member of the management team, in planning, problem resolution and reviewing the performance and compliance of functional areas;
- Provides guidance to Executive and Senior Managers on matters relating to Data Protection/Data Privacy, to include the DPA and attendant regulations and other relevant legislation;
- Participates in meetings, seminars, workshops, conferences, and other fora, as required;
- Prepares Annual/Quarterly/Monthly and other reports as required.

##### ***Technical/Professional:***

- Provides technical, legal and regulatory advice to senior management on data protection/data privacy issues, laws and trends;
- Drafts new and/or amends existing internal data protection/data privacy policies, guidelines, and procedures, in consultation with key stakeholder;
- Informs and advises employees who carry out processing of their obligations under the DPA and other relevant data protection policies and procedure provisions;
- Monitors compliance with the DPA and attendant regulations, other relevant data protection provisions, and the organisation's policies and procedures relating to data protection/data privacy, including how the organisation assigns responsibilities, raises awareness and trains staff involved in processing operations, and related audits;
- Ensures that any contravention of the data protection standards or any provisions of the DPA by the organisation is dealt with;
- Supports the organisation's contravention and security breach notification procedures;

- Co-operates with competent authorities and/or the OIC, responding to requests about complaint handling, investigations or inspections;
- Acts as the contact point for competent authorities and/or the OIC on issues relating to processing and consulting, where appropriate, with regard to any data protection related matter;
- Highlights or draws the organisation's attention to any failure to comply with the DPA and attendant regulations and applicable data protection/data privacy policies and procedures;
- Reports to the OIC where the organisation fails to rectify, within a reasonable time, any area of non-compliance with the DPA and attendant regulations which has been highlighted;
- Supports/manages a programme of awareness-raising and training to enable staff compliance and to foster a Data Protection/Data Privacy culture within the organisation;
- Trains and/or sensitises employees on the DPA's compliance requirements;
- Develops the relevant training material for dissemination;
- Conducts regular assessments and audits to ensure compliance with the DPA and attendant regulations;
- Serves as the point of contact between the organisation and the OIC;
- Consults with the OIC to resolve any doubt about how the provisions of the DPA and attendant regulations are to be applied;
- Ensures the conduct of risks assessments to, among other things, inform the preparation and submission of annual DPIAs to the OIC;
- Maintains records of relevant data processing activities conducted by the organisation.
- Assists data subjects in the exercise of their data protection rights;
- Handles queries or complaints received by responding to data subjects to inform them, among other things, about how their personal data is being processed and what measures the organisation has put in place to protect their data; and ensuring that requests are addressed in compliance with the DPA and attendant regulations;
- Keeps abreast of changes in the legislative environment and adjusts the organisations data protection/data privacy programme accordingly;
- Participates in security incident response procedures;
- Provides statements, attend court or tribunal proceedings and gives evidence, as required
- Provides reports in relation to various proceedings/hearings, as required;
- Performs miscellaneous duties related to job function, as required, from time to time.

### **Required Knowledge, Skills and Competencies**

#### ***Core:***

- Excellent written and oral communications skills;
- Leadership and management skills;
- Interpersonal and customer relations skills;
- Problem solving and analytical skills;
- Teamwork and co-operation skills;
- Judgment and decision-making skills;
- Consultation and issues management skill;
- Tact and diplomacy to manage issues with key stakeholders;
- Planning, organizing and time management skills;
- Stakeholder engagement, relationship management and networking skills;
- Negotiating skills;
- Integrity;
- Adaptability;
- Confidentiality;
- Ability to use own initiative.

#### ***Technical:***

- Sound knowledge of Data Protection/Data Privacy Laws and practices;
- Knowledge of international standards and best practices in Data Protection/Data Privacy Policy Development and Implementation;
- Knowledge of Data Security Systems;
- Ability to evaluate and assess business processes and business operations;
- Ability to communicate with and understand the requirements of professional staff within their area of specialization;
- Knowledge of current Data Protection developments/trends;
- Knowledge of Cybersecurity Risks and Information Security Standards;
- Proficient in the use of current/relevant computer applications especially Microsoft Office Suite (Word, Excel, PowerPoint).

### **Minimum Required Qualification and Experience**

- Graduate Degree in Law, Information Technology/Computer Science, Accounting, Risk Management or related discipline from an accredited tertiary institution;
- Three (3) years' of experience in Law, Information Technology/Computer Science, Audit or Risk Management or equivalent related experience;
- Knowledge of Data Protection/Data Privacy Law and Practices;
- Experience or specialised training in Records and Information Management Systems would be an asset;
- One (1) Data Protection/Data Privacy certification such as, CIPP, CIPT, CIPM, etc. (preferred).

#### **OR**

- Undergraduate Degree in Law, Information Technology/Computer Science, Accounting, Risk Management or related discipline from an accredited tertiary institution.
- Five (5) years' of experience in Law, Information Technology/Computer Science, Audit or Risk Management or equivalent related experience.
- Experience or specialised training in Records and Information Management Systems would be an asset.
- At least one (1) Data Protection/Data Privacy certification such as, CIPP, CIPT, CIPM, etc. (preferred).

### **Special Conditions Associated with the Job**

- May be required to travel;
- May be required to work beyond scheduled hours on weekends and public holidays, when the need arises.

Applications accompanied by résumés should be submitted **no later than Thursday, 26<sup>th</sup> September, 2024 to:**

**Senior Director  
Human Resource Development and Management Division  
Office of the Prime Minister  
1 Devon Road  
Kingston 10.**

Email: [jobs@opm.gov.jm](mailto:jobs@opm.gov.jm)

Please note that only shortlisted applicants will be contacted.

**Please ensure that a copy of this circular is placed at a strategic position on the Notice Board of the Ministry/Department/Agency and brought to the attention of all eligible officers.**



**Desreen Smith (Mrs.)  
for Chief Personnel Officer**