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
Website: www.osc.gov.jm

CIRCULAR No. 441 **11th November, 2024**
OSC Ref. C.6555[18]

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 2)** in the **Office of the Supervisor of Insolvency, Ministry of Industry, Investment and Commerce**, salary range $$4,266,270 - 5,737,658 per annum.

Job Purpose

Under the direct supervision of the Supervisor of Insolvency, the Data Protection Officer (DPO) will be responsible for:

- Designing and overseeing the implementation of an effective data protection framework (*complete with policies, procedures, guidelines and assessment mechanisms*), in keeping with the Data Protection Act and all other relevant legislation.
- Monitoring compliance with the OSI's and OGT's data protection measures through the creation of operational guidelines, the execution of audits, and the provision of recommendations for improvement, where necessary.
- Ensuring awareness of the data protection framework by all staff through the co-ordination of training and sensitization initiatives.

Key Responsibilities

Technical/Professional:

- Develops and implements frameworks for Data Protection, to include a policy, procedures, guidelines, and operational roadmap;
- Keeps abreast of changes in the legislative environment and adjusts the Agency's frameworks accordingly, to ensure consistency at all times;
- Develops audit approach and programmes on data security and protection;
- Conducts Department-wide data security and protection audits and makes recommendations towards the effective adoption of the legally prescribed implements by the OSI and the OGT;
- Conducts annual Protection Impact Assessment (DPIAs) to identify and mitigate risk-factors in the data protection process for the OSI and OGT;
- Consolidates the overall DPIA findings;
- Discusses DPIA findings with the Supervisor of Insolvency and Government Trustee on their respective offices;
- Creates annual report of the Data Protection Impact Assessment (DPIA) for submission to the Office of the Information Commissioner, Ministry of Science, Energy and Telecommunication;
- Assists both Departments and its relevant officers in preparation for audits which touch and concern Data Protection;
- Implements communication strategy to ensure the sensitization of all staff about the data protection policies and guidelines, the role of each employee in ensuring the Departments' compliance, and its value of the data protection mandate to the stakeholders of the OSI and OGT;
- Liaises with external data controllers that process data on behalf of the Departments, to ensure that the established data protection standards are upheld at all stages of the data lifecycle;
- Maintains a record of all external data controllers with whom both Departments do business;
- Engages with stakeholders to ensure privacy by design at all levels;
- Ensures all concerns raised by data subjects are addressed within legal timeframes;
- Ensures the security of audit files.

Human Resources:

- Ensures that data protection standards are observed in the undertaking of all human resource management related functions, including recruitment and selection, separation, and performance management processes;
- Creates and manages a data protection awareness programme for staff that includes;
  - ✓ Training sessions towards mastery of the Departments' data protection procedures on an individual level;

- ✓ Sensitization initiatives to educate staff about data protection best practices and regulatory requirements;
- ✓ Effective staff engagement on updates in the data processing and protection legal landscape.

Management/Administrative:

- Participates in the Departments' Strategic Planning Process;
- Participates in the development of the Operational and Annual Audit Work Plan;
- Provides day-to-day direction in the Departments' mission to fulfill its data protection mandate;
- Advocates for the establishment and maintenance of a culture of data protection and privacy within the OSI and the OGT;
- Ensures that all required processes, systems and controls are in place, to ensure adherence to the national Data Protection Standards in all areas throughout the OSI and OGT;
- Plans, organizes and co-ordinates inspections and audit intervention;
- Establishes effective partnership with external stakeholders with whom the Departments will collaborate to achieve its data protection mandate;
- Reviews existing policies, procedures and guidelines that have implications for data processing and makes recommendations to ensure that the data protection standards are upheld;
- Convenes meetings to discuss data protection issues and propose solutions, as required;
- Represents the Departments at meetings and seminars on Data Protection and Security;
- Creates annual report of the Data Protection Impact Assessment (DPIA) for submission to the Office of the Information Commissioner and the relevant Ministry;
- Prepares other reports and project documents, as required;
- Creates a Data Protection Committee and chairs same.

Customer Service:

- Maintains customer service principles, standards and measurements;
- Identifies and incorporates the interests and needs of customers in business process design;
- Ensures critical success factors are identified and meet expectations;
- Promotes customer trust and confidence in conducting transactions with the Departments by guaranteeing maximum protection of all personal and sensitive data;
- Prepares quarterly and annually Customer Service reports by established standards;
- Performs any other related duties that may be required from time to time.

Other:

- May be required to provide witness statements, attend Court proceedings, and give evidence;
- May be required to provide reports in relation to disciplinary proceedings non-Court Hearings.

<u>Required Knowledge, Skills and Competencies</u>

Core:

- Excellent leadership and people management skills;
- Excellent verbal and written communication skills;
- Excellent customer service and interpersonal skills;
- Excellent planning, organization, and time management skills;
- Strong analytical, judgement, decision-making and problem-solving skills;
- Ability to think strategically;
- Report writing skills;
- Keen attention to detail;
- Ability to work independently with minimal supervision;
- Ability to work in a team environment;
- Ability to adapt, especially under pressure;
- Ability to display high levels of confidentiality, integrity and professionalism;
- Ability to communicate, interact and work effectively and co-operatively with all people including those from diverse ethnic and educational backgrounds;
- Working knowledge of Supervisory practices and standards.

Technical:

- Advanced IT skills in the Microsoft Office Suite Applications;
- Working knowledge of the Insolvency Act and Regulation;
- Working knowledge of the Data Protection Act and other applicable regional, international data protection laws and regulations is required;
- Ability to understand and interpret complex legal requirements surrounding data privacy

is a definite asset;
- Detailed knowledge and understanding of international data protection best practices.

Minimum Required Qualification and Experience

- Master's Degree in Information Security, Computer Science, Information Technology, Management Information Systems, or a related field; **or**
- Bachelor of Laws Degree (LLB) and Certificate of Legal Education; **or**
- ACCA level 2 or, ACCA Fundamentals with more than two (2) years' experience or Bachelor of Science Degree in Accounting, Finance, Business Administration or Management Studies with Accounting from a recognized University; **or**
- ISO 27701 Approved Auditor;
- At least one 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 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)
- Five (5) years' work experience in Privacy, Compliance, Information Security, Auditing or a relevant field (Finance, Law, Business Administration, Information Technology);
- Two (2) years' work experience in mapping/understanding business processes and data handling needs in a relevant/related industry;
- Relevant working knowledge in cybersecurity – dealing with real security incidents, risk assessments, countermeasures and data protection impact assessments would be an asset; **or**
- Working experience in advising and auditing on matters of data and privacy compliance and enforcement, data breaches, data laws and other requirements; **or**
- Working experience in auditing/assessing compliance with data protection obligations, identifying data protection risks.

Special Conditions Associated with the Job

- Working outside the normal working hours in completing the Work Programme;
- Working on weekends, if required.

Applications accompanied by résumés should be submitted **no later than Friday, 22nd November, 2024 to:**

Director, Human Resource Management and Development
Ministry of Industry, Investment and Commerce
4 St. Lucia Avenue
Kingston 5

Email: hrm@miic.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