PROPOSAL

GOVERNMENT OF JAMAICA
DATA PROTECTION ACT (DPA)
COMPLIANCE FRAMEWORK FOR MINISTRIES, DEPARTMENTS AND AGENCIES (MDAs)

Version 1.2
June 2024

This document provides a guide to public authorities on the general requirements of the Data Protection Act and related Regulations, and outlines some considerations to ensure compliance. The document is not intended to replace knowledge of the Act and related Regulations.

Document Control

Owner:

Owner/Contributors
eGov Jamaica Limited - eGovJa
Office of the Information Commissioner - OIC
Office of the Prime Minister - OPM

Review Schedule:

This document shall be reviewed at least once annually or as deemed necessary.

Document Revision History

Version No.	Date	Author	Change Description
1.0	October 2023	eGovJa	First Release – drafted the document and submitted to ICT Division of the OPM and OIC for feedback.
1.1	January 2024	eGovJa	Incorporated feedback from the OIC.
1.2	May 2024	eGovJa	Removed DPO Job Description template and made other edits based on feedback from the ICT Division of the OPM, OIC and eGovJa

Contact Information

For further information about this document, contact the Office of the CEO at eGovJa or the Office of the Information Commissioner.

Table of Contents

Table of Tables

Abbreviations and Key Terms

Abbreviation	Change Description
DPA	Data Protection Act, 2020
DPIA	Data Protection Impact Assessment. This is a method for identifying and assessing privacy risks.
DPO	Data Protection Officer
eGovJa	eGov Jamaica Limited
GOJ	Government of Jamaica
MDAs	Ministries, Departments and Agencies
OIC	Office of the Information Commissioner
OPM	Office of the Prime Minister
PERSONAL DATA	Information relating to a living individual, or an individual who has been deceased for less than thirty years, who can be identified from that information alone or from that information and other information in the possession of or likely to come into the possession of a data controller
PROCESS	Obtaining, recording, or storing the information or personal data or carrying out any operation or set of operations (whether or not by automated means) on the information or data
PUBLIC AUTHORITY	A Ministry, department, Executive Agency or other agency of Government; a statutory body or authority, being a body corporate established by an Act of Parliament and over which the Government or an agency of the Government exercises control; a local authority within the meaning of the Local Governance Act; any company registered under the Companies Act, being a company in which the Government or an agency of the Government is in a position to direct to direct the policy of that company; a commission of parliament; or any other body or Public Authority which provides services of a public nature which are essential to the welfare of Jamaican society, or such aspects of their operations, as may be specified by the Minister by order published in the Gazette.
RIGHTS OF DATA SUBJECTS	Include rights to be informed about data processing, access their data, object to processing, request rectification not to be subject to automated decision-making and consent to be direct marketed | Includes, but is not limited to the right to be informed about data processing; right to access personal data; right to prevent processing; right to the rectification of inaccuracies; right not to be subject solely to automated decision-making; and a right to give and withdraw consent generally and specifically as it regards direct marketing [as outlined primarily at Part II of the DPA, ss. 5 to 13]
SENSITIVE PERSONAL DATA	Personal data consisting of any of the following information in respect of a data subject: genetic/biometric data; filiation or racial or ethnic origin; political opinions, philosophical beliefs, religious beliefs or other beliefs of a similar nature; membership in a trade union; physical or mental health or condition; sex life; or, the alleged commission of any offence by the data subject or any proceedings for any offence alleged to have been committed by the data subject.
TOR	Terms of Reference

1 TARGET AUDIENCE

This document is intended for use by any public authority staff as a general guide to ensure compliance with the ***Data Protection Act, 2020*** (DPA), the ***Data Protection Regulations, 2024***, the ***Data Protection (Data Controller Registration) Regulations, 2024,*** and any other Regulations, Codes of Practice and Guidance Notes issued under the DPA. This includes all public authorities, that is, Government Ministries, Departments and Agencies (MDAs), Local Government Bodies, Statutory Bodies, Regulatory Authorities, etc. These public authorities will play a vital role in ensuring that the personal information of data subjects is protected.

This document is not intended to replace knowledge of the DPA and Regulations, but rather will serve as a guide towards compliance.

2 INTRODUCTION

Given the recent passing of the DPA, public authorities must safeguard the personal information of data subjects and ensure that their constitutional right to privacy of personal data, including sensitive personal data, is protected. To do so, entities must have a robust data protection program designed and implemented. The aim is to ensure that data protection laws and regulations are followed while fostering a culture of privacy and security. This document provides some general considerations that will assist with meeting these objectives.

Considerations included herein are:

1. General methodology to ensure compliance with the DPA.
2. Data Protection Governance.
3. Proposed Data Protection Officer (DPO) staffing framework for the Government of Jamaica (GOJ) (in the short and medium term).
4. Sample Terms of Reference (TOR) for a consultancy engagement for a DPO as a service from a qualified firm, where applicable.

3 BACKGROUND

The DPA was passed in 2020 and seeks to establish a framework to protect the rights of data subjects. This legislation aims to regulate the processing of personal data, ensuring that it is done lawfully and transparently while safeguarding the rights and freedom of individuals. This was necessary to ensure that there was a structured way to treat with the following:

Protection of Privacy: To protect the privacy of individuals in a time when personal data is increasingly collected, processed, and stored by various entities and business organizations.

Regulation of Data Processing: To set clear guidelines and standards for how personal data should be handled and ensure that it is processed securely, fairly, and most importantly, lawfully.

Building Trust: The DPA helps build trust between individuals and the entities that process their data, by ensuring that the data is handled responsibly.

Compliance with other International Standards: Many countries have implemented similar data protection laws, for instance, the European Union General Data Protection Regulation (GDPR). Jamaica's DPA, therefore, aligns us with international standards and best practices regarding data privacy.

Data Subjects Rights: The DPA provides individuals with rights regarding their personal data, such as the right to access their data, the right to correct their personal data, and the right to prevent processing under certain conditions.

Data Security: The DPA mandates measures to protect data from unauthorized access, alteration, disclosure, or destruction, thereby enhancing data security.

Legal Framework for Data Breaches: The DPA establishes legal obligations for entities to report data breaches and outlines penalties for non-compliance or violations of the Act.

Economic Growth and Innovation: By creating a secure and structured way for personal data handling, the DPA encourages innovation and investment in digital services and technologies.

The DPA imposes certain responsibilities and obligations on data controllers, data processors, and other key actors, some of whom are:

Data Subject: A named or otherwise identifiable individual who is the subject of personal data, and in determining whether an individual is identifiable, account shall be taken of all means used or reasonably likely to be used by the data controller or any other person to identify the individual, such as reference to an identification number or other identifying characteristics which are reasonably likely to lead to the identification of the individual.

Data Controller: Any person or public authority, who, either alone or jointly or in common with other persons, determines the purposes for which, and the manner in which, any personal data are, or are to be, processed. Where personal data is processed only for purposes for which they are required under any enactment to be processed, the person on whom the obligation to process the personal data is imposed by or under that enactment is for the purposes of this Act a data controller. (The entity that determines how and why personal data is processed.)

Data Processor: Any person other than an employee of the data controller, who processes the data on behalf of the data controller. (An entity that processes data on behalf of the data controller.)

Information Commissioner: The office established pursuant to section 4 of the DPA to, among other things, monitor compliance with the DPA.

All MDAs and Public Bodies of the GOJ need to quickly fulfil compliance obligations under the DPA. This requires each entity to have a DPO to provide oversight of the DPA compliance. There are resource gaps in the current job market for DPOs since it is a relatively new job area. Further, it is impractical for all GoJ entities to quickly hire or contract the services of a DPO.

4 STEPS TOWARDS DPA COMPLIANCE

To properly protect the privacy and rights of individuals whose data the Public Authority processes, it is crucial to ensure compliance with the DPA. Given that this is a new area for most public authorities, it is imperative that there be a systematic approach to managing and safeguarding personal data within the Public Authority.

Public Authorities must follow data protection principles, implement adequate security measures, report breaches, conduct Data Protection Impact Assessments (DPIA) for high-risk processing, and, as stated previously, appoint a DPO.

The following 9-step methodology may be used as a ***guide***:

4.1 Get Familiar with the Requirements of the Act

Understand the requirements and provisions of the DPA and the areas that will be relevant to the Public Authority;

4.2 Conduct a Data Audit and Mapping

Conduct a thorough assessment of all the processes within the Public Authority that collect, process, store, and share personal data, along with the purposes for each data category. Ensure that a data inventory is created to understand how all personal data item flows through the Public Authority, and further that data is classified according to sensitivity;

4.3 Conduct a Risk Assessment

Once a clear picture is derived of how personal data flows through the Public Authority, identify the privacy risks with each personal data item. This assessment should include an infrastructure security scan for various systems and the Public Authority's security network. A Risk Management Plan should be developed to mitigate or control identified risks and ensure compliance with the DPA;

4.4 Develop and Implement Data Protection and Privacy Policies and Procedures

Develop and implement the required policies and procedures that align with the requirements of the DPA. These policies and procedures must outline how the Public Authority should collect, process, store, and share personal data. Also, consideration

must be given to the rights of the data subjects, the disposal processes, and the security measures that will be executed to safeguard personal data items and the process to handle breaches;

4.5 Conduct Staff Training and Awareness

Establish a training program for all employees to raise awareness about the DPA, the importance of compliance, and the policies and procedures approved for implementation.

Ensure also that all data privacy team members are sensitized on the DPA, and the data privacy standards as required under the Act;

4.6 Conduct Regular Compliance Assessments

These assessments, to include Business Impact Assessment and Privacy Impact Assessment, will ensure that the Public Authority is adhering to the defined policies and procedures and thus complies with the provisions under the DPA. The policies and procedures must be updated, as needed, to address any compliance matters;

4.7 Appoint a Data Protection Officer

As per the DPA, an appropriately qualified DPO must be appointed who will be responsible for monitoring, in an independent manner, the data controller's compliance activities in relation to the DPA. The appointment of the DPO shall be in keeping with the criteria as provided in section 20 of the DPA, regulation 9 of the Data Protection Regulations, 2024 and any information and/or guidelines that may be issued under the Act;

4.8 Register With the Office of the Information Commissioner

Register with the OIC as a data controller and update registration annually and particulars as necessary (i.e., when details have changed);

4.9 Ensure Compliance with the Data Protection Standards

The DPA places specific emphasis on eight (8) Data Protection Standards that must be met, these are summarized as follows and may further be understood at https://oic.gov.jm/page/data-protection-standards:

1. Fair and lawful processing
2. Limited purposes for data processing
3. Data minimization
4. Accuracy of data
5. Storage limitation
6. Rights of The Data Subject
7. Implementation of Technical And Organizational Measures
8. Cross-Border Transfers

It is also important to document the steps to be taken to handle a personal data breach, or contravention of any of the above, including communication to internal and external parties such as the:

a) OIC to report a breach or a contravention within 72 hours;
b) Jamaica Cyber Incident Response Team, Jamaica Constabulary Force or Major Organised Crime and Anti-Corruption Agency (e.g., for cyber threats/incidents and cybercrimes, etc. which may require investigation);
c) Affected data subjects to notify them of a breach which may place them at additional risk;
d) General public to communicate standardised responses to contain a situation and provide updates as necessary;

The entity must also familiarize itself with the consequences of non-compliance as stated in the DPA. For example, the imposition of fines and terms of imprisonment on any individual found culpable for breaches or contraventions of the Act.

For a detailed analysis and comprehensive understanding, it is recommended to refer directly to the DPA.

Refer to the **Data Privacy and Protection Checklist** in Appendix 7.1 for additional guidance.

5 PROPOSED GOVERNANCE

Data protection governance is important for the Public Authority to ensure that data protection laws and regulations are effectively managed and adhered to. The governance structure would generally include the following:

a) Define roles and responsibilities for data governance within the organisation
b) Recruitment or assignment of a **Data Protection Officer**
c) Establishment of a **Data Protection Working Committee**, with defined roles and responsibilities
d) Define and implement **Training and Awareness Programs**
e) Establishment of **Policies and Procedures**
f) Conduct regular **Audits and Assessments**

As per regulations, the DPO must "report to a person, or persons, at the senior management or executive management level within the data controller's organisational structure". The DPO must ensure that reports on data protection matters are developed and submitted to the Board of Directors or Head of the Public Authority (as the case may be) on an agreed cadence.

The governance structure must be reviewed and adjusted as needed to reflect new regulatory requirements and the changing needs of the Public Authority.

Please refer to the proposed Staffing Guideline for further insight into the roles and responsibilities of the key players.

6 PROPOSED GOJ DPO STAFFING GUIDELINES

According to the DPA, a DPO must be named by a public authority. The DPO can be linked to a new post created on the Public Authority's structure or a role assigned to an existing employee with the requisite aptitude and skillset to execute the defined functions. The functions may also be outsourced and shared with other Data Controllers, in accordance with Regulation 9 of the Data Protection Regulations, 2024.

Nevertheless, to determine what is best suited for a Public Authority, consideration must be given to the complexity and influence of the Public Authority, which includes the following:

1. The size of the Public Authority
2. The industry
3. The data processing activities
4. The compliance requirements

Given the aforementioned, and the specific needs of the Public Authority, the below staffing framework may be considered for options.

6.1 Establish a Data Protection Team

A Data Protection team generally includes representation from the roles in the table below. If, however, these roles are not on the existing Public Authority structure and the Public Authority is not in a position to recruit, the team selected should collectively have experience and skills in all domains.

Role	Description
DPO	• Responsible for monitoring compliance with the DPA and ensuring compliance to all documented policies and procedures. • Consult on DPIAs, etc. • Conduct training where required • Serve as a contact point for data subjects and regulatory authorities.

Role	Description
	• Develop and submit reports on data protection matters to the Board of Directors or Head of the Public Authority (as the case may be) on an agreed cadence.
Legal Expert	• Provide legal advice on data protection issues, review contracts and agreements related to data processing activities, and also ensure the Public Authority's compliance with relevant laws and regulations.
Information Technology (IT) Security Specialists	• Implement technical measures for data protection, conduct security assessments, and ensure the security of data processing systems and infrastructure.
Human Resource Management	• Ensure that employees are adequately trained on data protection policies and procedures and maintain records. • Ensure that a training program is established for continuously raising awareness about the DPA and compliance imperatives.
Privacy Champions	• Support the implementation of privacy related/impacting initiatives. • Assist with sensitizing staff to training and awareness campaigns. • Assist with ensuring that staff understand the Data Protection related policies and procedures.
Support Staff	• Any other support staff from within the Public Authority that is required to contribute to the compliance, revision or development of policies and procedures.

Table 1 Sample Data Protection Team

6.2 Appoint a Data Protection Officer

As stated above, this role is required under the DPA. Considerations for the acquisition of a DPO may be any of the following options:

- contractual engagement for DPO services (see sample Terms of Reference in Appendix 7.2) OR
- an established post on the public authority's approved Establishment OR
- shared with other Data Controllers in accordance with Regulation 9 of the Data Protection Regulations, 2024.

Public Authorities should consider also the complexity and/or sensitivity of their business processes and data to determine whether to engage their own DPO. See the table below.

BUSINESS PROCESS COMPLEXITY	PROPOSED DPO MODEL	EXAMPLES
High or Sensitive	Assigned/discrete DPO within the Ministry serving all or most entities, being on staff or contracted For the entity, DPO on staff OR DPO as a Service	• Ministry of Finance and the Public Service • Ministry of National Security /Jamaica Constabulary Force • Jamaica Defence Force • eGovJa • Tax Administration Jamaica • Jamaica Customs Agency • National Housing Trust • Registrar General's Department • Accountant General's Department • National Health Fund
Low-Medium	Shared DPO within the Ministry serving all or most entities, being on staff or contracted	• Jamaica Information Service • Office of Utilities Regulation • Child Protection and Family Services Agency • National Insurance Scheme

Table 2 GoJ DPO Staffing Matrix

6.3 Establish the Reporting Structure

It has been a firm recommendation that the internal DPO be treated akin to an audit related function, though being a separate role from the Internal Auditor. The DPO must report to a person, or persons, at the senior management or executive management level within the data controller's organisational structure to ensure the scope, autonomy and independent action to effectively execute these duties within the Public Authority. The DPO will also be able to report to the Board of Directors, on data protection activities, identify risks, and raise compliance matters.

7 APPENDICES

7.1 DATA PRIVACY AND PROTECTION CHECKLIST

Data Privacy and Protection Checklist		
	Done?	**Comments**
1. Owner/Sponsor of the Data Protection Program identified Head of Entity/CEO/Managing Director appoints a lead within the organisation	☐	
2. Review the Data Protection Act and note requirements	☐	
3. Identify the internal Data Protection Compliance Team 3.1. Data Protection Officer 3.2. Data Privacy Analysts/Privacy Champions 3.3. Legal Expert 3.4. IT Security Specialist 3.5. Compliance Officer	☐ ☐ ☐ ☐ ☐	
4. Establish an appropriate Data Privacy governance structure.	☐	
5. Resolution of the Board of Directors/Directive of Head of Entity received establishing the Data Protection project team and documented Charter.	☐	
6. Assess the financial capacity of the Public Authority to recruit a consulting firm to lead the Data Protection Compliance Program.	☐	
7. Determine if a budget is available to recruit a Data Protection Officer.	☐	
8. Develop a Charter for governing the working committee or project team 8.1. Include the selected team members 8.2. Include the identified Privacy Champions 8.3. Obtain board or Head of Entity approval for the documented Charter	☐	
9. Conduct an As-Is assessment/Data Audit and Mapping 9.1. Document all the processes that collect, process, store, and share personal data 9.2. Document how the personal data for each item flows within and outside of the Public Authority	☐	

Data Privacy and Protection Checklist		
	Done?	**Comments**
9.3. Conduct a Data Privacy Impact Assessment to determine how the Public Authority currently complies with the Act; document all non-conformities to be addressed. *(To identify, understand and communicate the nature of processing conducted by the Public Authority and to identify areas of inefficiencies, non-compliance, and opportunities for improvement.)*		
10. Develop a Data Protection Awareness Training Programme for staff	☐	
11. Conduct an Information Security Management System Audit to identify non-conformities on the Public Authority's digital infrastructure.	☐	
12. Process developed to monitor non-conformities and track the progress of unresolved issues	☐	
13. Develop and implement policies and procedures to ensure compliance with the defined Data Protection Standards	☐	

7.2 DPO CONSULTANCY TERMS OF REFERENCE (TOR)

1. OBJECTIVE OF THE ASSIGNMENT

The Consultant will provide <***ENTITY***> with Data Protection Officer (DPO) services to ensure ongoing compliance with the Data Protection Act. The specific objectives of the assignment include:

- Independent monitoring and ensuring <ENTITY>'s compliance with the requirements of the DPA and all applicable laws and regulations related to data privacy and data protection;
- Serving as the primary point of contact within the organisation for members of staff, regulators, data subjects and any relevant public bodies on issues related to data privacy and data protection;
- Ongoing review of policies that enforce compliance with applicable legislation; and
- Providing training to staff to increase awareness of data privacy and protection requirements.

2. SCOPE

The scope of work is not considered exhaustive and modifications will be considered during the course of the engagement. All changes to the scope of work shall be formally agreed upon by both parties. The scope of work includes:

a. Identify opportunities to enhance <ENTITY>'s Data Protection/Privacy Programme.
b. Identify all laws, regulations, standards, and contracts that impose compliance obligations on <ENTITY> related to data privacy or data protection.
c. Ensure that <ENTITY> processes personal information in compliance with all applicable laws, regulations, standards, and contracts and in accordance with industry best practices.
d. Evaluate the effectiveness of <ENTITY>'s data protection framework and ensure that areas of non-conformance with applicable legislation are escalated to the appropriate officers for corrective action.
e. Lead and direct internal reviews to ensure compliance with applicable standards and address potential issues.
f. Work with project teams to ensure compliance with applicable legislation/regulations, ensure privacy by design and conduct privacy impact assessments where necessary.
g. Recommend to the CEO corrective measures necessary to address areas of non-compliance with <ENTITY>'s data privacy and data protection obligations and monetary fines/penalties applicable.
h. Assist data subjects in the exercise of their rights under applicable legislation concerning personal data collected or processed by <ENTITY>.
i. Consult with the Information Commissioner.
j. Act as a contact point for data subjects and the Office of the Information Commissioner (OIC).

k. Develop and report on KPIs to measure <ENTITY> compliance with data privacy/data protection obligations.
l. Ensures awareness of and adherence to the Human Resource Policy, Circulars, Staff Orders and other policies and management procedures within the organisation; that are relevant to the Data Protection Act and the obligations thereunder.
m. Develops and executes training programmes to ensure that staff of <ENTITY> maintain awareness of policies, standards and guidelines related to data privacy and data protection.
n. Manage all identified nonconformities to ensure that root causes are determined and corrective actions implemented.

3. METHODOLOGY

The Consulting Firm is expected to use accepted and proven methodologies for carrying out the assignment. The Consulting Firm should prepare a detailed work plan indicating how the objectives and scope of the assignment will be achieved.

The work plan submitted should be supported with a Work Breakdown Structure and a Schedule showing the allocation of time to each of the key components of the assignment.

4. COORDINATION/REPORTING RELATIONSHIP

The Consulting Firm will report to and operate under the supervision of the CEO or designate. The CEO/designate will coordinate the monitoring, review, and approval of the documents prepared by the Consulting Firm.

5. DELIVERABLES

The deliverables under this assignment are directly linked to the agreed scope of work. The specific deliverables included are specified below:

- Updated data protection policies and procedures;
- Management of nonconformities;
- Maintenance of records of processing activities;
- Data protection training and awareness;
- Data subject rights management;
- Incident response plans, including notification procedures for data breaches;
- Evaluation of the data protection practices of third-party vendors;
- Compliance reports prepared for Executive Management and the OIC as necessary;
- Regular audits of data protection processes and practices;
- Data Protection Impact Assessments including maintenance required documentation;
- Guidance on embedding privacy by design principles within the Public Authority's projects and processes.

All documents submitted must conform to the following minimum standards:

- Should follow the draft outline that is to be submitted to, and approved by the Department Head before the deliverable is formally submitted;
- Should use language appropriate for a non-technical audience;
- Should be comprehensive, properly formatted and well-presented;
- Should provide justifications for all assumptions.

5.1. "Sign-off" Procedure

The CEO will work with the Consulting Firm to ensure the deliverables align with the objective of this assignment. It is also expected that the Consulting Firm will present the deliverables to various units as the need arises.

5.2. Variations

All proposed changes to the work plan and associated deliverables must be discussed with the CEO, and where necessary must be submitted for approval.

5.3. Schedule of Payment

Payments for the services will be specified in the Contract.

6. QUALIFICATION AND TECHNICAL EXPERTISE REQUIRED

6.1. The Consulting Firm

The Consulting Firm should have the following minimum qualifications:

1. At least two (2) years experience in data protection/ data privacy practice;
2. Submit two (2) client references relating to data protection/ data privacy projects

6.2. Key Skills/ Qualifications of the Data Protection Officer/Key Personnel

The key subject matter expert(s) assigned by the consulting firm to this engagement should have the following minimum qualifications and demonstrate the following competencies:

1. Bachelor's Degree, preferably in Computer Science or Law Degree from a recognised institution (preferred)
2. Experience with ISO 27001 & ISO 27701 implementation (preferred)
3. Data Protection or Privacy certification such as CIPP, CIPM, CDPSE (preferred)
4. Extensive knowledge of the Data Protect Act 2020
5. Five (5) years of experience within a compliance, legal, audit or risk function, with recent experience in privacy compliance
6. Experience in conducting Data Protection Impact Assessments (DPIAs)
7. Must be fluent in English.

6.2.1. Personal Attributes and Characteristics of the Assignment

1. Strong project management skills and an ability to work collaboratively with diverse teams and stakeholders
2. Professional maturity and interpersonal skills to navigate relationships with wide-ranging stakeholders
3. Sound professional judgment, integrity, discipline, and respect for all colleagues and stakeholders
4. Detailed-oriented with the ability to work effectively without supervision and to take responsibility for end-to-end delivery to the client

7. CHARACTERISTICS OF THE CONSULTANCY

Type of consultancy:	Consulting Firm
Duration of Contract	Executed over 12 months
Place of Work:	Jamaica, at <ENTITY> Offices
Type of Contract:	Timed Based Contract
Payment Responsibility	<ENTITY>
NB: The contract amount includes all costs related to undertaking the consultancy.	

8. EVALUATION CRITERIA

	Evaluation Criteria	**Maximum Points**
1.	***Adequacy of Experience of the Consultancy Firm for the Assignment***	**30**
	1.1 At least two (2) years experience in data protection/ data privacy practice • 2 years' experience or more [15 marks]; or • 1 year or more but less than 2 years of experience [10 marks]; or • Less than 1 year's experience [5 marks]; or • No experience [0 marks] 1.2 Submit two (2) client references relating to data protection/ data privacy projects • Participating bidders should have the Client Referral Forms (CRF) completed and submitted along with their submission, as points will be awarded to the average Quality of Service (QoS) score for all two (2)	30

	Evaluation Criteria	Maximum Points
	client referral forms. Please see the Section 3 – Standard Forms for the CR template. Scores will be allocated as follow: • QoS average score of 23-28 – 15 points • QoS average score of 17-22 – 10 points • QoS average score of 11-16 – 5 points • QoS average score below 11 – 0	
2.	***Adequacy of Qualification and Experience of the Data Protection Officer/Key Personnel for the Assignment***	**70**
	2.1 **Qualification of Data Protection Officer**: a) Bachelor's Degree in Computer Science or Law Degree from a recognised institution (preferred) [20 marks]; b) Data Protection or Privacy certification such as CIPP, CIPM, CDPSE [10 marks]; c) Experience with ISO 27001 & ISO 27701 implementation [5 marks]; d) Extensive knowledge of the Data Protect Act 2020 or a similar legislation (for example GDPR) [5 marks];	40
	2.2 **Data Protection Officer** – Experience within a compliance, legal, audit or risk function, with recent experience in privacy compliance a) 5 years experience or more [20 marks]; or b) 3 years or more but less than 5 years of experience [15 marks]; or c) 2 years or more but less than 3 years experience [10 marks]; or d) Less than 2 years experience but greater than 1 year [5 marks]; or e) No experience [0 marks]	20
	2.3 **Data Protection Officer** - Experience in conducting Data Protection Impact Assessments (DPIAs) a) 2 or more years of experience [10 marks]; or b) Less than 2 years experience but greater than 1 year [5 marks]; or c) Less than 1 year [0 marks]	10
	Total	**100**

NB: Only candidates who have attained the minimum score of 70 points or more will be considered for contract award.

If there still exists a tie after the evaluation exercise, the contract will be awarded to the first submitted proposal of the bidders that are tied.