



## REQUEST FOR PROPOSAL (RFP) FOR DATA PROTECTION IMPACT ASSESSMENT AND POLICY IMPLEMENTATION

### Invitation to Submit Proposal

11<sup>th</sup> December 2023

### Subject: RFP for KAM DATA PROTECTION IMPACT ASSESSMENT AND POLICY IMPLEMENTATION

You are requested to submit a proposal for the provision of the above-referenced subject. Your proposal could form the basis for a contract between your firm and the Kenya Association of Manufacturers (KAM).

To enable you to submit a proposal, please find enclosed:

- a) Annex I: Terms of Reference (TOR), containing a description of KAM requirements for which these services are being sought.
- b) Annex II: Proposal submission: Description of requirements for proposal submission.

In case you need clarification on the RFP kindly feel free to contact us through [procurement@kam.co.ke](mailto:procurement@kam.co.ke). We will be more than willing to share and clarify any query regarding the project. Kindly make sure you have the words **DATA PROTECTION IMPACT ASSESSMENT AND POLICY IMPLEMENTATION** in the subject of the email.

#### Note:

This letter is not to be construed in any way as an offer to contract with your firm/ institution.

Yours Sincerely,

A handwritten signature in black ink, appearing to read 'Anthony Mwangi', written over a circular stamp or seal.

**Anthony Mwangi**  
Chief Executive



## **ANNEX I**

# **TERMS OF REFERENCE FOR DATA PROTECTION IMPACT ASSESSMENT AND POLICY IMPLEMENTATION**

## **INTRODUCTION**

The Kenya Association of Manufacturers (KAM) was established in 1959 as a private sector body and has evolved into a dynamic, vibrant, credible, and respected business membership association that unites industrialists and offers a common voice for businesses.

KAM provides an essential link for cooperation, dialogue, and understanding with the Government by representing the views and concerns of its members to the relevant authorities. In pursuit of its core mandate of policy advocacy, KAM promotes trade and investment; upholds standards; and encourages the formulation, enactment, and administration of sound policies that facilitate a competitive business environment and reduce the cost of doing business.

## **OBJECTIVE**

To be compliant with the Kenya Data Protection Act 2019 and its Regulations, organizations must ensure that they have the appropriate policies, procedures, and technical measures in place to protect personal data. KAM seeks to put in place a comprehensive data protection policy, classification framework and compliance monitoring framework and impact Assessment tools. KAM is therefore seeking the services of a consultant to conduct data protection impact assessment (DPIA) to inform the development of a Data Protection policy.

## **TERMS OF REFERENCE**

KAM currently does not have a data protection policy in place. In line with the implementation of the Data Protection compliance application, the consulting company will also be required to assist with coming up with and implementing a Data Protection Policy for the Association in line with the Kenya Data Protection Act, 2019 once the DPIA has been conducted.

## **Scope of Work for Data Protection Impact Assessment (DPIA) under the Kenya Data Protection Act 2019**

### **1. Introduction**

The purpose of this Data Protection Impact Assessment (DPIA) is to assess the potential risks and impact on data protection associated with specific data processing activities as required by the Kenya Data Protection Act 2019. The DPIA will be conducted following the Act's provisions and guidelines issued by the Data Protection Commissioner.

### **2. Objectives**

Identify and describe the data processing activity to be assessed.  
Evaluate the necessity and proportionality of data processing.  
Assess the potential risks and impact on data subjects' rights and freedoms.  
Propose measures to mitigate identified risks and ensure compliance with the Kenya Data Protection Act.

### **3. Data Processing Activity**

Describe the specific data processing activity, including the purpose, nature, scope, and context of the processing. Identify the types of personal data involved, data subjects, and any third parties involved in the processing.

#### 4. Data Protection Principles

Assess the adherence to the principles outlined in the Kenya Data Protection Act, including lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.

#### 5. Necessity and Proportionality

Evaluate the necessity and proportionality of the data processing for the stated purpose. Determine whether the data processing is the least intrusive means of achieving the intended purpose.

#### 6. Risks and Impact Assessment

Identify and assess the potential risks and impact on the rights and freedoms of data subjects. This includes the likelihood and severity of risks such as unauthorized access, data breaches, data inaccuracies, and other privacy-related concerns.

#### 7. Mitigation Measures

Propose and outline measures to mitigate identified risks and ensure compliance with data protection requirements. This may include technical, organizational, or procedural measures to enhance data security and protect data subjects' rights.

#### 8. Consultation and Involvement

Describe the process of consultation with relevant stakeholders, including data subjects, if applicable. Highlight any concerns raised during the consultation process and how they have been addressed.

#### 9. Documentation and Record-Keeping

Ensure that all aspects of the DPIA process are documented comprehensively. Maintain records of the assessment, including methodologies, findings, and mitigation measures.

#### 10. Review and Monitoring

Establish a framework for ongoing review and monitoring of the data processing activity to ensure continued compliance with data protection requirements. Outline the frequency and procedures for periodic reviews.

#### 11. Reporting

Prepare a comprehensive DPIA report, including a summary of the assessment, findings, recommended mitigation measures, and any other relevant information. Submit the report to the Data Protection Commissioner and relevant stakeholders as required by the Act.

#### 12. Compliance Certification

If applicable, provide a compliance certification indicating that the data processing activity has been assessed, and measures have been implemented to ensure compliance with the Kenya Data Protection Act 2019.



## **POLICY CREATION AND IMPLEMENTATION**

The consultant will be required to develop a comprehensive Data Protection Policy for Kenya Association of Manufacturers (KAM), ensuring compliance with the Kenya Data Protection Act 2019. This policy will provide clear guidelines on the collection, processing, storage, and sharing of personal data to protect the rights and privacy of data subjects.

### **SCOPE**

#### **1. Policy Development Team**

Identify and assemble a cross-functional team, including legal, IT, HR, and other relevant stakeholders, to collaborate on the development of the Data Protection Policy.

#### **2. Legal and Regulatory Compliance Review**

Conduct a thorough review of the Kenya Data Protection Act 2019 to ensure that the policy aligns with the legal and regulatory requirements outlined in the legislation.

#### **3. Stakeholder Consultation**

Engage with key stakeholders, including legal counsel, management, IT, HR, and other departments to gather insights and ensure the policy reflects the organization's specific needs and considerations.

#### **4. Policy Scope and Objectives**

Clearly define the scope and objectives of the Data Protection Policy, outlining its applicability to all personal data processed by the organization and the overarching goal of ensuring compliance with the Kenya Data Protection Act.

#### **5. Data Processing Principles**

Incorporate the data protection principles outlined in the Kenya Data Protection Act, such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality into the policy.

#### **6. Data Subject Rights**

Define and explain the rights of data subjects as per the Act, including the right to access, rectify, erasure, object, and restrict processing. Detail the procedures for data subjects to exercise their rights.

#### **7. Data Security Measures**

Specify the technical and organizational measures in place to ensure the security and confidentiality of personal data, including encryption, access controls, and regular security assessments.

#### **8. Data Breach Response and Notification**

Establish procedures for detecting, reporting, and responding to data breaches, including the notification process to the Data Protection Commissioner and affected data subjects, as required by the Kenya Data Protection Act.

#### **9. Data Protection Officer (DPO) Role and Responsibilities**

If applicable, outline the role and responsibilities of the Data Protection Officer, including their contact information and reporting structure within the organization.

#### **10. Training and Awareness Programs**

Develop and implement training programs to ensure all employees are aware of their responsibilities under the Data Protection Policy and receive training on data protection principles and best practices.

#### **11. Data Processing Impact Assessment (DPIA)**

Integrate the requirement for DPIAs into the policy, outlining the circumstances under which a DPIA is required and the procedures for conducting and documenting such assessments.

#### **12. Policy Review and Updates**

Establish a regular review process to ensure the Data Protection Policy remains current and compliant with any changes in legislation, technology, or organizational processes.

#### **13. Communication Plan**

Develop a communication plan for the rollout of the Data Protection Policy, including training sessions, awareness campaigns, and clear communication channels for employees to seek clarification.

#### **14. Policy Approval and Implementation**



Present the drafted Data Protection Policy to the executive team for review and approval. Develop an implementation plan for the organization-wide rollout of the policy.

## **Methodology**

The consultant shall follow one of the agile methodologies of project management. The rapid module development is expected to create iterations with the users and continuous feedback that helps with faster project delivery. The best part of this methodology is short time boxes, known as iterations, which happen to last from one week to one month.

## **APPROACH**

The company will work under the direction of the ICT and legal department. KAM will provide any required information to the contracted company as necessary.

## **TIME SCHEDULE AND LEVEL OF EFFORT**

The assignment will be carried out over a period of **1 to 2 months**. The period can be extended by KAM ICT Manager if deemed necessary.

## **ANNEX II**

### **Manner of submission**

1. Your proposal shall be prepared in the English Language
2. Your proposal shall comprise the following documents:
  - a) Technical component and
  - b) Financial (price component)
3. Your proposal shall be prepared in duplicate with one marked "original" and the other marked "copy". In the event of any discrepancy between them, the original shall govern.
4. Please insert dates and addresses as necessary.

## **Content of Proposal**

### **I. Technical Component**

- i. Description of the firm and the firm's qualifications (company profile).
- ii. Copy of Company Certificate of incorporation
- iii. Statutory KRA PIN and VAT certificate copies
- iv. Up-to-date tax compliance certificate
- v. Brief description of Understanding of the requirements for services, including assumptions.
- vi. Proposed approach and methodology/Clear project plan.
- vii. The consultant should be compliant with the Kenya Data Protection Act 2019, and regulations 2021 and provide proof of compliance.
- viii. Proposed team structure.
- ix. Proposed project team members and their qualifications (At least one (i) member of the team **must have a** Legal background with experience in Kenya data privacy laws and regulations, and any ICT degree with Cybersecurity qualifications and experience.



- x. Audit experience to be able to systematically assess an organization's data infrastructure, policies, and processes against the Kenya Data Protection Act, 2019 requirements.
- xi. Security expertise, including risk management, cybersecurity concepts, and data breach response plans.
- xii. Knowledge of relevant information technologies like data mapping/tracking tools, encryption, and analytics, that enable compliance with the Kenya Data Protection Act 2019 and regulations 2021.
- xiii. Understanding of The Kenya Data Protection Act, 2019, regulations 2021 scope, key principles like data minimization and individual rights, and specific obligations for controller vs processors.
- xiv. Experience in carrying out Data Protection Impact Assessments (DPIA)
- xv. Demonstrate experience implementing Data Protection Act programs and protections in a variety of organizations (at least 2).

## **2. Financial (Price Component)**

- i. A summary of the cost.
- ii. The period of its validity.
- iii. Taxes

### **Payment terms (provisions)**

Kenya Association of Manufactures policy is to pay for contractual services based on the performance of contractual services rendered. **For this task, KAM intends to make all payments upon completion of the assignment.**

### **Evaluation of proposals**

A two-stage procedure will be utilized to evaluate the proposals, with an evaluation of the technical component completed before any price component. Scores will be awarded for the technical proposal. The price component proposal will be opened only for those firms/ institutions whose technical component meets the requirements for the assignment, as indicated by a score of more than 70%.

### **Deadline for Submission**

The proposals are to be submitted for the attention of the Procurement Unit, **KAM House 5<sup>th</sup> floor. 15 Mwanzi Road, Opp Westgate Mall by 22<sup>nd</sup> December, 2023, at 12.00 p.m. Late submissions will not be opened.**

**Please Label the Envelope “DATA PROTECTION IMPACT ASSESSMENT AND POLICY IMPLEMENTATION”**