DATA PROTECTION COMPLIANCE AND IMPACT ASSESSMENT

1. INTRODUCTION

Financial Sector Deepening Kenya (FSD Kenya) is an independent trust dedicated to the achievement of a financial system that delivers value for a green and inclusive digital economy while improving financial health and capability for women and micro and small enterprises (MSEs).

We work closely with the public sector, the financial services industry, and other partners to develop financial solutions that better address the real-world challenges that low-income households, micro and small enterprises, and underserved groups such as women and youth face.

FSD Kenya was established in 2001 to support the development of inclusive finance as a means to stimulate wealth creation and to reduce poverty. In 2005, FSD Kenya was constituted as an independent trust. We operate under the supervision of professional trustees with policy guidance from a programme investment committee (PIC).

Our current funders are FCDO, the Swedish International Development Cooperation Agency (SIDA), and the Bill & Melinda Gates Foundation.

FSD handles a lot of data at different levels, and in line with the Data Protection Act (DPA) 2019, requires the services of a firm to provide consulting services, working closely with the FSD team to ensure full compliance with the DPA and the General Data Protection Regulation (GDPR). This will among others include undertaking an audit and impact assessment of the status, develop necessary processes for implementation ensuring compliance.

2. OBJECTIVES

The identified firm/consultant will ensure FSD Kenya complies with the Data Protection Act of 2019 and GDPR, review all FSD Kenya processes to ensure they are compliant with the requirements. The firm will train FSD staff on data protection awareness and develop tools to implement Data Protection policies as well as identify all contract templates that need to be modified to meet the new requirements of the DPA and assist to modify the contracts accordingly.

3. SCOPE OF WORK

The firm will carry out the following tasks:

3.1 Conduct Data Audit.

Map the FSD's input and output data. The data sets to be audited are not limited project data, data collected for research, staff personal data and FSD Kenya stakeholders' data. Demarcate the data sets between personal and non-personal data. Clearly identify the data sets that fall under the purview of Kenya's Data Protection Act 2019 (DPA). Develop a data inventory template that will be adopted and updated by FSD Kenya.

3.2 Data Privacy Governance Assessment

The firm will conduct an assessment on FSD's data privacy practices and policies to ensure that they follow Data Protection Act of 2019 and are aligned with privacy principles. The assessment should rate FSD Kenya's compliance based on maturity model/ rating scale (ISO 15504) against the 14 privacy principles of:-

1. Choice and Consent
2. Legitimate Purpose & Use Limitation
3. Personal Data Life Cycle
4. Personal Data Accuracy & Quality
5. Openness, Transparency and Notice
6. Individual participation
7. Accountability
8. Personal Data security and Safeguards
9. Monitoring, Measuring and Reporting
10. Prevent Harm
11. Third-Party/Vendor Management
12. Breach Management
13. Privacy by Design/Data Security
14. Data Transfers/ Free Flow of Information

3.3 Drafting of policies, procedures, and contract clause templates
Review all FSD Terms of Use and Privacy Policies and make recommendations to enhance Compliance with the Data Protection Act (2019) and the Data Protection policy and guidelines. Advise appropriate cookie policies and implementation actions. Develop data sharing consent processes and templates and advise on how they may be digitally implemented.

3.4 Assist in the implementation of data protection
Review FSD systems and data stores for safe use and processing of data and recommend configuration of such privacy and sensitivity tags.

3.5 Contract Modification
The firm will assist in the modification of FSD's data protection contract clauses in line with the Data Protection Laws in conjunction with FSD's legal advisor.

3.6 Data Protection Impact Assessment
Perform impact assessment on FSD high risk data processing activities.

3.7 Staff Awareness Training
The identified firm will conduct staff training on privacy awareness to ensure all staff members understand the importance of data privacy and to familiarise themselves with the main concepts and requirements of the DPA and GDPR. The training should be moulded in accordance with its audience and adapted to their needs by linking the legal frameworks with FSD Kenya's business operations. The training should emphasize staff duties and responsibilities with regards to existing policies and importance of compliance.

4. CONDUCT OF THE WORK

The firm will be supervised by the COO and Operations Manager, who will coordinate with

relevant stakeholders for provision of required the content and guidance on the desired output. Close engagement will be required throughout the assignment. This will be coordinated by the IT Team in conjunction with the FSD Kenya DPIA audit project team.

Note that all data, information, and materials accessed and prepared during this assignment, shall remain confidential and under the care of FSD Kenya. A Non-Disclosure Agreement will be signed by the consultant. Any of the data and material shall not be used for any other purpose other than for the reason of this engagement.

5. OUTCOMES AND DELIVERABLES

The firm is expected to deliver the following:

1. Staff awareness training

The vendor will conduct 1.5-hour privacy awareness training to enable the management and employees to understand the importance of data privacy and to familiarise themselves with the main concepts and requirements of the DPA and GDPR.
The training will be moulded in accordance with its audience and adapted to their needs by linking the legal frameworks and the FSD's operations. It should also inform the staff of their duties and responsibilities with regards to existing policies.

2. Data Protection Implementation.
3. Ensure FSD Kenya is registered and compliant with Data Protection Act 2019.
4. Customisation of Data Protection Documentation
5. Recommend configuration FSD Kenya systems for compliance.
6. Contracts such as controller to processor agreement, data sharing agreement, cross-border processor agreement.
7. Data Protection awareness training materials
8. Policies such as Privacy Policy, Record Management policy, Data Subject Access Request Policy, Data Breach Response Plan

The copyright for all material prepared under these terms of reference will pass to FSD Kenya. It is FSD's practice to publish the reports it commissions in its own house style. There is therefore no requirement for material to be extensively formatted beyond that required to indicate how material should be logically presented in the final report. All final reports should be presented in an electronic format allowing the text and graphics to be manipulated in preparation for publication. Where a final report is presented in a portable document format (pdf) generated from another format (such as Microsoft Word) it should be accompanied by the original file from which it is generated. All representations of graphic material (tables, figures, drawings, charts, graphs and photographs) must be able to be reproduced at high print resolution. Tables, figures, drawings, charts, graphs should be provided in Microsoft Excel or Adobe Illustrator format. Photographs must be provided in high-resolution JPG images set to minimum of 300 dots per inch (dpi). Any technical questions regarding these requirements should be addressed to FSD's Communications Officer.

6. REQUIREMENTS

Mandatory requirements
A well-established firm with a good track record of working on providing Data Protection advisory services in Kenya and the wider region.
Knowledge of Data Protection Act (DPA) and the General Data Protection Regulation (GDPR)
Proven experience in developing privacy compliance policies
Verifiable proof of previous engagements in similar assignments
At least two years' experience in conducting Data Audit, Data Protection Impact Assessment (DPIA) and recommending configurations to systems and technology to prevent data leakage.

7. EVALUATION CRITERIA

Assessment criteria	Weighting (%)
Experience of the Consultant/firm	
A well-established firm with a good track record of working on providing Data Protection Consulting services in Kenya and the wider region for at least two years.	20
Content, quality, and completeness of the proposal – Demonstratable understanding of the TORs	10
Approach and methodology	
Solid knowledge and demonstrated experience in conducting Data Audit, Data Protection Impact Assessment, and providing training and actionable insights on the outcome of the reviews including methods and tools that will be used with three letters of reference.	20
Staff schedule, work and deliverable schedule	
Adequacy of the proposed staff schedule to meet the needs of the ToR	10
Responsiveness of proposed work plan in relation to the ToR	10
Key Professional Personnel Qualification for the Assignment **Note: Bidders to respond in relation to the Key personnel requirement and evaluation criteria in this section**	
Responsiveness of the CVs to the requirements of the ToR	10
Financial Evaluation The formula for determining the financial scores is the following: FS = S% x LB/BP where: FS = financial score LB = Lowest/Most competitive bid BP= Cost of the bid been considered S% = Percentage score The weights given to the Technical (T) and Financial (F) Proposals are: T = 80% and F = 20%	20
Total	**100%**

FSD Kenya will undertake a due diligence assessment and screening of the preferred Bidder to include reference checks. FSD Kenya will share a Third-party screening questionnaire to aid in processing the assessment and screening. FSD Kenya reserves the right to proceed or reject Bidder(s) depending on the outcome of this assessment and consider the next ranked bidder. The findings of this assessment will be kept confidential and used internally for the purposes of this evaluation.

FSD Kenya reserves the right to accept any tender (s) or to reject all tenders at any time. FSD Kenya also reserves the right to cancel this procurement at any point in time prior to award of the contract.

If you would like to lodge a complaint in regard to this procurement process, please write to tenders@fsdkenya.org with the address **data protection compliance and impact assessment**. FSD Kenya procurement team will acknowledge receipt of the complaint in writing within three (3) working days.

During the course of this procurement if you come across any issues of bribery, corruption or wrong doing on FSD Kenya part, please feel free to contact Julius Anyega, FSD Kenya Chief Operations Officer at Julius.Anyega@fsdkenya.org or transparency@fsdkenya.org

8. SUBMISSION

Interested bidders should send proposals by email to tenders@fsdkenya.org on or before **March 20th, 2023, at 17:00HRS (EAT)** with the subject line **"data protection compliance and impact assessment"** If you have any clarification questions, please email us at tenders@fsdkenya.org no later than 8th March 2023. Responses to clarification questions shall be sent on 10th March 2023.

Tender security is NOT required. Issuance of this request for proposals in no way obligates FSD Kenya to award a contract. Applicants will not be reimbursed for any costs associated with their application.

9. TIMETABLE

The Data Protection Compliance work will be carried out for a period of two months from the signed contract start date. The firm will provide Data Protection awareness sessions, one session at the completion of the contract, and the next, 3-4 months later.