

# Balozi Co-operative Savings and Credit Society Ltd.



Invest in secure hands

Golf View Suite, 3rd Floor, Wambui road off Kiambu/Thika road

P.O. Box 11539 – 00400, Nairobi, Kenya.

Tel: 020-2211600 Cell: 0720-833326 / 0733-967707

Email: info@balozisacco.com Website: www.balozisacco.com

2<sup>nd</sup> July 2024

Dear Sir/Madam,

## **RE: ADVERTISEMENT FOR DATA PROTECTION SERVICES**

Balozi Sacco is a non-WDT Sacco regulated by SASRA with its office in Nairobi. The Sacco has a membership of over 4000 and asset base of over Ksh. 5 billion. The Sacco is registered as a Data Controller and a Data Processor by the Office of the Data Protection Commissioner (ODPC).

The Sacco seeks to **engage a partner to act as the Sacco's data protection officer** and to provide services endeared to the implementation of the Data Protection Act, 2019 and Regulations.

### **Objectives**

The key objectives include and not limited to:

1. Correspondence with Office of the Data Protection Commissioner (ODPC), relevant Regulators, and other key stakeholders on behalf of the Sacco.
2. Assist and guide staff & Management in responding to enquiries or requests from Regulators (ODPC) on regards to data subjects and other stakeholders as appropriate.
3. Organize and participate in the training and awareness programs for staff on the relevant data protection & privacy requirements and obligations.
4. Promote a culture of data protection & privacy by design and by default in the Sacco.
5. Review of data mapping for all personal data in the custody of Sacco.
6. Review of data protection impact assessment.
7. Review of consent management & breach notification.
8. Review of data protection policy for any updates.
9. Review of management of third-party documents, data processors and transfer of personal data
10. Review of data retention management
11. Provide quarterly monitoring and evaluation assessment reports on data protection services.

### **Data Protection firm**

Balozi Sacco will only engage organizations registered with the ODPC and who have prior similar experience. The key personnel should also be registered with an approved professional body to act as the Data Protection Officer for organizations.

## **Scope of work / Key responsibilities**

1. Ensure licenses with the office of the data protection commission (ODPC) are up to date.
2. Review and maintain data protection policies and procedures. Regularly monitor compliance with policies.
3. Review vendor contracts to ensure that the Sacco interests are protected in terms of data protection.
4. Negotiate, review and draft data sharing agreements with new suppliers.
5. Guide in data mapping for all personal data in the custody of the Sacco.
6. Prepare guidelines and conduct a data protection impact assessment including a risk assessment to identify gaps in the Sacco in relation to the Act and policies for data held by the Sacco. Ensure that DPIA measures are implemented.
7. Conduct inspections and periodical audits of the processes and systems of data controllers and data processors.
8. Implement/enforce recommendations on gap analysis in line with data.
9. Oversee the maintenance of records required to demonstrate data protection compliance.
10. Facilitate adoption and testing of the data retention policy.
11. Develop a process to periodically audit personal data retained/disposed within the Sacco.
12. Research and keep abreast of any changes to relevant laws and regulations and prepare regular updates to management and the board.
13. To facilitate the identification and resolution of challenges associated with implementation and maintenance of the Data Protection Act and regulations compliance activities.
14. Creating awareness to internal stakeholders on the requirements, expectations and impact of the Data Protection Act and regulations.
15. Guide management in ensuring that an appropriate and comprehensive information governance framework is in place and being developed throughout the Sacco.
16. Assist in development of Information Governance Toolkits which will enable in conducting assessments, report incidences, and create continuous awareness amongst stakeholders.
17. Formulation of a framework for detection, reporting and investigation mechanisms for data breaches.
18. Support data incident response and data breach notification procedures.
19. Receive and process notifications of data breaches from Data Controllers and Data Processors
20. Creation of a framework for third party due diligence and data protection audits.
21. Personal data inventory (identification of personal identifiable information).
22. Serve as the point of contact between the Sacco and the Regulatory Authorities.
23. Provide regular status updates to management and draw immediate attention to any compliance risks and/or exposure to the applicable data protection rules.
24. Ensure that all systems and procedures comply with all relevant data privacy and protection regulations.
25. Conduct reviews to ensure compliance and accountability and proactively address potential issues.
26. Maintain a data security incident management plan for timely remediation of incidents.
27. Prepare inspection and compliance reports.
28. Reviewing evidence submitted by Data Controllers and Data Processors relating to information, privacy and security safeguards for cross-border data transfers.

29. Provide monitoring and assessment reports on a quarterly basis and advise the management on the best practice.
30. Any other relevant deliverables not indicated above.

### **Deliverables and Outputs**

- a. Detailed Data Protection Impact Assessment (DPIA) report with a corrective action plan (Gap analysis report and resolution measures).
- b. Information Governance Toolkits for conducting self-assessments.
- c. Development of a compliance road map, consisting of steps to bring the Sacco into compliance with the applicable data protection laws and regulations.
- d. Data loss business continuity plans.
- e. Quarterly monitoring and assessment report.
- f. Any other deliverable not included above.

### **Consultant Qualifications**

The Consultant should have skilled key personnel in the following fields (proof must be provided):

- Experience in undertaking Data Protection Assessments in the Financial Services Sector
- Experience in undertaking Data Protection Implementation
- Experience in provision of Data Protection Training
- Experience in reviewing Data Mapping

### **Certifications Requirements**

Certified Data Privacy Solutions Engineer (CDPSE), Certified Information Privacy Professional (CIPP), Certified Information Privacy Manager (CIPM), Certified Information Security Manager (CISM), Certified Data Protection Officer (CDPO or GDPR).

The team should at least comprise of an ICT consultant with a bachelor's degree in IT related field in combination with data protection certifications and, a legal consultant with at least an LLB or Business/Risk/Compliance consultant with a bachelor's degree in a relevant business field and experience in Regulatory compliance.

### **Duration of engagement**

The firm will be required to prepare an activity schedule that will take care of all phases of the assignment, i.e., document review, field work and assembling of information and writing the reports. The engagement will be for a period of one year.

### **Remuneration and terms of payment**

20% down payment on signing of contract and the balance pro-rated upon successful completion of the implementation milestones as per an approved checklist.

### **References**

You are required to attach written proof of recommendation on similar services offered from at least 3 referees of which at least one must be a Sacco.

### Criteria for evaluation

| Description   | Score   |
|---|---|
| Attach certificate of incorporation   | Yes/No<br><br>Mandatory documents<br><b>(Failure to attach any required document will lead to disqualification)</b> |
| Attach current trade license  |   |
| Attach current tax compliant certificate  |   |
| Proof of registration with ODPC   |   |
| Lead team to have an ICT consultant with a degree in IT related field. Attach academic proof.   |   |
| Lead team to have a legal consultant with an LLB or Business/Risk/Compliance consultant with a bachelor's degree in a relevant business field and experience in Regulatory compliance. Attach academic proof. |   |
| Attach written recommendations / proof of service from 3 referees for similar data protection services  |   |
| <b>Evaluation Criteria</b>  |   |
| Proposal submitted meets the scope of work  | 15  |
| Experience of the firm in providing similar consultancy services. Attach proof of 3 latest similar services completed for similar engagement with at least one being a Sacco (5 marks for each)               | 15  |
| Education level and professional qualifications of key personnel.   | 20  |
| Cost = $CI/Cc \times M$ .<br>Where,<br><b>CI</b> is Lowest quote received<br><b>Cc</b> is the Quote of Consultant being evaluated<br><b>M</b> is the total score for cost (30 marks)                          | 50  |
| Total   | 100   |

### Submission of proposal and quotation

Your proposal and quotation marked "Data protection services" should be dropped in our tender box at the reception by 5.00 pm on **Wednesday 10<sup>th</sup> July 2024**.

Yours Faithfully,



Jorim Oyago  
Chief Executive Officer