KENVERSITY COOPERATIVE SAVINGS AND CREDIT SOCIETY LIMITED

P.O. BOX 10263 – 00100
NAIROBI.

TELEPHONE: 020 812782 / 020 8002371, 020 8002372.

EMAIL:info@kenversitysacco.co.ke
www.kenversitysacco.co.ke

TENDER DOCUMENT PROVISION OF DATA PROTECTION MANAGEMENT SYSTEM

PROVISION OF DATA PROTECTION MANAGEMENT SYSTEM

KENV/TNDR/DTM/2025

KENVERSITY COOPERATIVE SAVINGS AND CREDIT SOCIETY LIMITED

CONDITIONS OF TENDERING

Serial No. …….

Miscellaneous Receipt No. ……

Date of Receipt …… Amount in Kshs.. ……

1. **DEFINITIONS**

The Tenderer is the person who undertakes to supply the goods/services described in the tender documents.

The signatory must be a recognized official of the company and be authorized to sign on its behalf.

2. DOCUMENTS

2.1 The tender will receive a miscellaneous receipt of payment for tender documents. These include the following forms in duplicate:

(i) **Form of tender**
(ii) **Conditions of tendering**
(iii) **Confidential business questionnaire,**

The Tenderer should retain one set for his records and return the other set in accordance with these conditions.

2.2.1 The Tenderer is required to check the number of pages of the document accompanying the **form of Tender**. Should any be missing or any figure indistinct, or should there be doubt about the precise meaning of any item or figure for any reason whatsoever he/she must inform the tender issuing officer at once and have the matter rectified as required before the final date for submission of tenders.

2.2.2 The Tenderer's signature to all documents shall indicate that he/she fully understands their contents and that he/she accepts all the conditions stated or applied therein.

3. SUBMISSION OF TENDERS

3.1.1 Attention is invited to the tender notice. The complete tender documents must be submitted to the address shown on the form of tender in a sealed plain envelope endorsed on the out cover with **Tender for provision of Provision Of Data Protection Management System**. Indication of Tenderer's names/mark should not appear on the envelope.

3.1.2 The form of tender must be properly signed in ink, dated and must accompany any other documents concerned with the tender.

3.1.3 The tender will not be accepted unless correctly submitted on the approved forms. Tenders for which the appropriate fee has not been paid will not be considered valid. Tender shall be

deposited in the Tender box at **Kenversity Sacco Office** not later than the appointed time and date.

4.0 COMMUNICATION

4.1.1 There shall be no verbal variations in regard to a tender once submitted. Should an error be made it may be corrected in writing **before the closing date**.

4.1.2 All correspondence with the Tenderers will be sent to the address shown on the form of tender by post.

1 Liability

No liability will be admitted nor claim allowed for error in the tender owing to mistakes in those documents, which should have been rectified in the manner, described above.

2 Acceptance

The society reserves the right to accept or reject any tender either wholly or in part and is not bound to accept the lowest or any tender or to give reason for rejection.

3 Successful Tenderers

A letter of acceptance will be sent to the successful Tenderer in respect of the whole or that part of tender, which has been accepted within a validity period of 90 days.

COMPLIANCE WITH GIVEN CONDITIONS

CURRENT TRADE LICENCE NO._____EXP. DATE:_____
V.A.T. REG. NO._____
PIN NUMBER:_____
NAME OF YOUR AUDITORS: _____
OTHER GOVERNMENT STATUS: _____

COMPANY STAMP

If a Tenderer does not comply in any way with these conditions where necessary, the tender shall be liable to rejection.

Tenderer's Name ----------

Tenderer's Signature ----------

Designation ----------

Full address ----------

Telephone Number (office) ----------

Email ----------

Fax ----------

Date ----------

Official stamp/seal.

Name of the Building ---------- Plot No. ---------- Door No. ----------

Company Rubberstamp ---------- Date ----------

Telephone number ----------

Are you a Kenyan, if not, state your Nationality ---------- -

Name and address of your bankers ---------- -

Bankers certificate on the Tenderer's Liquidity, suitability, and credit limitation ---------- -

Bankers signatory – Manager/Accountant ---------- Date ---------- -

CONFIDENTIAL BUSINESS QUESTIONNAIRE

You are requested to give particulars indicated in Part I and part 2 as is applicable in your type of business. You are advised that false information/particulars will result in automatic disqualification and render the tender void.

Part 1 – General

Business Name ----------

Location of business premises ----------

Plots number ----------Street/Road----------

Postal Address ----------

Telephone number ----------

Nature of business ----------

Registration number ----------

Trade license Number ---------- Date of Expiry ----------

Maximum value of Business you can handle Kshs ----------

Name of your bankers ----------

Branch/address ----------

Part 2 Registered company

Private or Public ----------

State the normal and issued capital of the company:

Normal Kshs…….

Issued Kshs……..

Details of the Directors:-

Name	*Nationality/citizenship*	*Shares*
1. ----------	----------	----------
2. ----------	----------	----------
3. ----------	----------	----------

Date: ---------- Signature of Tenderer ----------

Official stamp ----------

If Kenyan citizen, indicate under "citizenship Details" whether by birth, nationalization or registration.

In the event of this tender being accepted in part or in full within the stipulated 90 days, I/We agree to supply against an order signed by an authorized officer of the Society and failure to do so will constitute breach of contract.

Tenderer's Name ----------

Tenderer's Signature ----------

Designation ----------

Full address ----------

Telephone Number (office) ----------

Email ----------

Fax ----------

Date ----------

Official stamp/seal.

Tenderer's name in full ---------- Signature ----------

Address ----------

Telephone number ----------

A. SCOPE OF WORK

THE SOLUTION

The Automation of Data Protection solution will provide the following fundamental capabilities:

1. Data Discovery and Classification: Automated identification and classification of sensitive data across diverse environments to ensure compliance and enhance protection measures.
2. Policy Management: Creation, management, and enforcement of consistent data protection policies across all repositories and applications.
3. Data Encryption: Automated encryption of data at rest, in transit, and during processing to safeguard sensitive information.
4. Access Control and Identity Management: Implementation of role-based access controls to ensure that only authorized personnel can access sensitive data.
5. Backup and Recovery Automation: Automated scheduling and management of backups, along with streamlined recovery processes to minimize downtime in case of data loss.
6. Threat Detection and Response: Continuous monitoring for anomalies or threats to data integrity, with automated response mechanisms to mitigate risks.
7. Audit and Compliance Reporting: Generation of automated reports to demonstrate compliance with regulations (e.g., Kenya Data Protection Act 2019, GDPR) and facilitate audits.
8. Incident Response Automation: Pre-defined workflows for responding to data breaches or incidents, enabling rapid containment and mitigation.
9. Data Masking and Tokenization: Techniques to protect sensitive data in non-production environments through masking or tokenization.
10. Integration Capabilities: Seamless integration with existing systems, applications, and cloud services for a unified data protection strategy.
11. User Education and Awareness: Tools to educate users on data protection practices and risks, fostering a security-oriented culture.
12. Scalability and Flexibility: Ability to scale and adapt to evolving data environments, ensuring robust protection as the organization grows.
13. Cost Management: Insights and automation for optimizing data protection costs, including storage management and resource allocation.
14. Multi-Cloud and Hybrid Support: Comprehensive data protection across multiple cloud providers and

hybrid environments.

15. Data Lifecycle Management: Automation of data retention, archival, and deletion processes to manage data through its lifecycle in compliance with policies and regulations.
16. Data Breach Handling: Procedures for reporting and tracking data breaches to ensure swift response and accountability.
17. Data Subject Access Request Automation: Streamlined processes for managing data subject access requests efficiently.
18. Risk Assessment: Data protection and privacy risk assessments, including identification, mitigation, and monitoring of controls.
19. Consent and Preference Management: Tools for managing user consent and preferences related to data processing.
20. Personal Data Inventory: Maintenance of a record of processing activities and data flow maps for transparency and compliance.
21. Compliance Checks: Regular tracking of compliance gaps and implementation of necessary corrective measures.
22. Third-Party Risk Assessment: Evaluation of risks associated with third-party vendors and service providers.
23. Cross-Border Data Transfer Management: Mechanisms to ensure compliance with regulations regarding cross-border data transfers.
24. Document Management: Effective management of documents related to data protection policies and procedures.
25. Data Privacy e-Learning: Availability of e-learning content to educate staff on data privacy and protection best practices.

FUNCTIONAL SPECIFICATION

The solution should strive to provide the following features. The bidder should clearly indicate whether the functionality is currently available or not.

1.1 THIRD PARTY PRIVACY RISK ASSESEMENT

Automation of Data Protection solutions must supply capabilities for assessing and managing privacy risks associated with third-party relationships. This entails evaluating third-party privacy practices, data handling procedures, and compliance with relevant privacy regulations. The solution should enable the identification of privacy risks, implementation of risk mitigation measures, and continuous monitoring and reporting to ensure third-party compliance with privacy regulations and contractual obligations.

1.2 DATA PROTECTION COMPLIANCE CHECKS AND GAPS TRACKING

The solution must provide functionality for conducting regular compliance checks against relevant data protection regulations and internal policies. The solution should identify gaps in compliance, prioritize remediation efforts, and track the status of corrective actions. Additionally, it should offer reporting capabilities to monitor compliance progress and demonstrate adherence to regulatory requirements.

1.3 DATA FLOW MAPS AUTOMATION

The solution must be capable of creating and visualizing data flow maps, illustrating the movement of personal data within and across systems. The solution should enable the identification of data sources, processing activities, and data recipients, facilitating transparency and accountability in data handling practices. Additionally, the system should support updates to data flow maps to reflect changes in data processing activities over time, aiding in compliance efforts and risk management.

1.4 PERSONAL DATA INVENTORY.

The solution should create and maintain a comprehensive inventory of personal data assets across the organisation's systems. This includes features for data discovery, classification, mapping, and documentation. The system should enable tracking of data flows, storage locations, and usage purposes, facilitating compliance with regulatory requirements and supporting data governance initiatives.

1.5 USER CONSENT AND PREFERENCE MANAGEMENT

The solution should enable effective management of user consents and preferences regarding data processing activities. This includes features for capturing, storing, and updating consent records, as well as mechanisms for users to easily review and modify their preferences. The system should also support compliance with relevant regulations, such as GDPR, by facilitating transparent communication and providing audit trails for consent changes.

1.6 DATA PROTECTION AND PRIVACY RISK MANAGEMENT

The solution must include comprehensive privacy risk management tools that enable proactive identification, assessment, and mitigation of privacy risks associated with personal data processing. It should offer capabilities for continuous risk monitoring, reporting, and recommendations for risk reduction strategies, ensuring compliance with Kenya and global data protection regulations.

1.7 DATA SUBJECT ACCESS REQUEST RIGHTS

The solution be able to automates the management and fulfillment of Data Subject Access Requests (DSARs), ensuring timely response within legal timeframes. The system should streamline request verification, data retrieval, and communication processes, while maintaining a log for audit purposes and compliance verification.

1.8 DATA BREACH MANAGEMENT

The system should be capable of data breaches management, include tools for incident response and forensic analysis, and ensure compliance with legal requirements for breach notification. The solution should support detailed reporting and continuous improvement to adapt to evolving threats and regulations.

1.9 DATA PROTECTION REPORTING AND ANALYTICS

The solution should offer robust reporting features to highlight critical data protection items and facilitate trend analysis. This includes generating reports on key metrics such as data breach incidents, compliance status, and privacy risk assessments. The solution should support trend analysis to identify patterns, emerging risks, and areas for improvement over time, aiding in strategic decision-making and proactive risk management efforts. The system should incorporate a report wizard; a graphical tool that will help users without technical expertise to create custom reports. it provides a step-by-step interface to define report layout, data sources, filters, and grouping options.

1.10 ABILITY TO INTERGRATE WITH EXISTING SYSTEMS

Supplier to demonstrate experience in integrating data protection solutions with existing IT infrastructure and business applications, ensuring seamless operation and minimal disruption.

1.11 ADMINISTRATOR PORTAL & DASHBOARDS

The system should provide user friendly administration portal to support backend operations by Bank personnel. The system should offer customizable dashboards that present real-time insights and visualizations inform of graphs, pie charts etc. Support customizations (to view only relevant data) and drilldowns based on role and span of control.

1.12 TWO-FACTOR AUTHENTICATION

The system should allow for a two-factor authentication process. The system should trigger OTP codes through SMS or/and e-mail. The system should monitor and control active sessions to prevent unauthorised access. Support for mobile app online push authentication (2FA) and offline authentication.

1.13 ACCOUNT ACCESS RECOVERY

The system should provide a secure and reliable account recovery option for users who have lost their 2FA device or cannot access it. The system should implement limits on account recovery attempts and introduce configurable delay times and/or account lockdown/cooldown period between unsuccessful attempts. This will help in preventing brute-force attacks. The system should have the ability to reset passwords using the registered e-mail address or phone numbers. The system should support multiple stringent verification processes that require users to provide multiple pieces of identity information before initiating the account recovery process. Methods such as e-mail verification, phone number verification, security questions and

recovery codes etc. can be used.

A. REQUIREMENTS

Interested bidders are therefore invited to respond and provide:

The ideal provider should also meet the following requirements:

1. Evidence of 5 years' experience in data protection application system services.
2. Include CVs of key staff that would be involved in the project.
3. Include details of a contact person.
4. Provide the Know your Client (KYC) required document - MANDATORY.
5. Detailed proposal as per the above scope of work
6. Itemized financial proposal.
7. Detailed company profile

B. TENDER PRICE AND CURRENCY

Prices quoted by the tenderer shall be fixed during the tender validity period and not subject to variation on any account. A tender submitted with an **adjusted price quotation** will be treated as non-responsive and will be rejected. The Price quoted shall be in the Kenya Shilling currency.

KNOW YOUR CLIENT (KYC) REQUIREMENTS FOR THIRD PARTIES	
SOLE PROPRIETOR	1. Copy of Business Registration 2. Copy Business Permit 3. Individual KRAPIN 4. KRA Tax Compliance Certificate 5. Bank details 6. Copy of Utility Bill or Lease to confirm existence of the Business premises 7. Client list of ongoing assignment. Provide contracting document and/or reference letters. 8. Audited Financial Statements for the last 24 months
LIMITED LIABILITY COMPANY	1. Copy of the certificate of incorporation 2. Copy Business Permit 3. KRA PIN certificate 4. KRA Tax Compliance Certificate 5. Copy of CR12 6. Bank details 7. Copy of Utility Bill or Lease to confirm existence of the Business premises 8. Client list of ongoing assignment. Provide contracting document and/or reference letters. 9. Audited Financial Statements for the last 24 months

PARTNERSHIPS	1. Copy of Partnership Deed /OR Affidavit 2. Copy of Certificate of Registration 3. Copy of Business Permit 4. KRA PIN certificate 5. KRA Tax Compliance Certificate 6. Letter signed by all the partners(on company letterhead) indicating mandates to transact business on behalf of the firm. 7. Copy of Utility Bill or Lease to confirm existence of the Business premises 8. Bank details. 9. Copy of Utility Bill or Lease to confirm existence of the Business 10. Client list of ongoing assignment. Provide contracting document and/or reference letters 11. Audited Financial Statements for the last 24 months