REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

When replying please quote
Ref: ODPC/DPC/CON/7 (74)

Britam Tower
P.O. Box 30920 - 00100
NAIROBI

Email: compliance@odpc.go.ke

17th July 2025

The Managing Director
Murang'a Water and Sanitation Company
Off Kangema Road
P.O Box 1050 - 10200
MURANG'A

Email: managingdirector@muwasco.co.ke

Dear MD,

RE: DATA PROTECTION AUDIT REPORT AND REQUEST FOR ROADMAP ON IDENTIFIED GAPS

Reference is made to our Audit Notice dated 11th September 2024, wherein the Office of the Data Protection Commissioner (ODPC) notified your organisation of its intention to conduct an audit and requested the provision of specified documents pursuant to its mandate and powers under Section 8 and Section 23 of the Data Protection Act, 2019 (Act).

Enclosed with this letter is the Audit Report prepared following the audit conducted by the Office. The report provides a detailed assessment of your entity's data protection practices, focusing on the following scope areas:

- Data protection governance and accountability
- Staff data protection training and awareness
- Security of personal data
- Data subject's rights requests
- Records management

MURANG'A WATER & SANITATION COMPANY LIMITED
07 AUG 2025
RECEIVED
P. O. Box 1050-10200, MURANG'A

KENYA VISION 2030

- Data Protection Impact Assessments (DPIAs) and information risk management
- Data sharing
- Vendor management
- Cross border transfer

The audit identified several gaps in these areas that require immediate attention to achieve compliance with the Act and its attendant regulations.

In light of the above, the Office requests that your entity develop a feasible and reasonable roadmap to address the gaps identified in the enclosed report. The roadmap should include:

1. A comprehensive plan detailing the steps your organisation intends to take to rectify each identified gap.
2. Realistic timelines for the implementation of these actions, including key milestones.
3. Details of any additional resources or support necessary to effectively address these gaps.
4. Provide for any considerations that the Office may need to take into account in reviewing the said roadmap.

Please submit your proposed roadmap to the Office no later than **6th August 2025**.

Further to the foregoing, our team remains available to discuss any questions or concerns you may have regarding the audit findings. In the meantime, should you require any clarification, please do not hesitate to contact the Office by email through compliance@odpc.go.ke.

Yours Sincerely,

Immaculate Kassait, MBS
DATA COMMISSIONER

REPUBLIC OF KENYA

OFFICE OF THE DATA PROTECTION COMMISSIONER

MURAN'GA WATER AND SANITATION COMPANY LIMITED (MUWASCO)

DATA PROTECTION COMPLIANCE AUDIT REPORT

DATE OF REPORT: 17TH JULY 2025

For: DATA PROTECTION COMMISSIONER
P. O. Box 30920-00100,
NAIROBI

TABLE OF CONTENTS

1 Executive Summary

Murang'a Water and Sanitation Company Limited (MUWASCO) was established under the Companies Act Cap 486 (Revised 2015) of Kenya and licensed by the Water Services Regulatory Board (WASREB). It provides vital water and sanitation services to Murang'a Municipality and its environment. Operating within a service area of approximately 350 km^2, MUWASCO manages three water treatment plants—Kiawambeu, Kayahwe, and Gakoigo, with a combined production capacity of 23,000 m^3 daily. The company also operates the Karie wastewater treatment plant, which treats 3,000 m^3 of wastewater daily. With a service population of about 120,000 residents, MUWASCO supports 19,000 active water connections and 6,500 sewage connections, achieving service coverage of 73% across its jurisdiction.

The Office of Data Protection Commissioner ('the Office') engaged MUWASCO to perform a data protection audit. This is as per Section 23 of the Data Protection Act and Regulation 53 of the Data Protection (General) Regulation of 2021, which mandates the Office to conduct compliance audits and periodic inspections of data controllers and processors to ensure compliance with the Act and regulations in Kenya.

This report outlines the findings and recommendations from the data protection compliance audit carried out by the Office on MUWASCO between 25th and 27th March, 2025, at the premises in Murang'a. The primary objective of the audit was to assess MUWASCO's compliance with the Data Protection Act, 2019, and its subsidiary regulations, and to ensure that MUWASCO has incorporated sound data protection measures, thus aiding them to meet their obligation under the Act. The audit examined key areas, including data processing practices, privacy safeguards, data security measures, staff training and awareness, and existing policies and procedures.

The Data Protection Auditor engaged MUWASCO to perform a data protection audit, this is a per Section 23 of the Data protection Act ("the Act") and Regulation 53 of the Data protection (General) Regulation of 2021 that mandates the office to carry out compliance

audit and periodic inspections of data controllers and data processors to ensure compliance with the Act. The audit was designed to evaluate MUWASCO's compliance with the Data Protection Act, 2019, and its subsidiary regulations and to ensure that MUWASCO has incorporated sound data protection measures, thus aiding them to meet their obligations under the Act.

The audit evaluated MUWASCO's adherence to Kenya's data protection laws and regulations. It covered various aspects of data processing, privacy measures, data security, training, awareness, and policies. This report presents the findings and recommendations from the data protection compliance audit conducted by the Office on MUWASCO from March 25th to 27th,2025.

This Data Protection Audit Report (report) outlines the findings and recommendations from the data protection compliance audit carried out by the auditor on MUWASCO on 25th, 26th, and 27th March 2025

The primary objective of the audit was to assess MUWASCO's compliance with the Data Protection Act, 2019, and its subsidiary regulations and to ensure that MUWASCO has incorporated sound data protection measures in its processes, therefore meeting its obligations under the Act. The audit examined key areas including data processing practices, privacy safeguards, data security measures, staff training and awareness, and existing policies and procedures.

2 Summary Findings

Areas of Compliance

MUWASCO has designated a Data Protection Officer (DPO), who concurrently serves as the head of the ICT department. Additionally, departmental heads have been appointed as data protection champions. However, MUWASCO has not complied with Section 24(6) of the Act, which mandates the publication of the DPO's contact details on the institution's website and formal notification to the ODPC. Moreover, the DPO has not been issued a

formal appointment letter, resulting in ambiguity regarding their official mandate, scope of authority, and functional responsibilities.

Areas for Improvement

1. Registration as a data handler with the Office of the Data Protection Commissioner. MUWASCO should initiate the registration process with the Office of the Data Protection Commissioner (ODPC) as a data handler (controller and processor).
2. Formal Appointment of a Data Protection Officer (DPO)
   - MUWASCO should formally appoint a DPO by issuing an official appointment letter.
   - The letter must define clear roles and responsibilities, ensuring no conflict of interest.
   - Publish the DPO's contact details on the MUWASCO official website and submit the information to the Office of the Data Protection Commissioner.
3. Data Mapping and Records of Processing Activities (RoPA)
   - Conduct comprehensive data mapping across all departments.
   - Document all categories of personal data, provide descriptions for each, and identify the lawful basis relied upon for collection.
4. Data Protection and Cybersecurity Training
   - Develop and implement a training schedule and training materials.
   - Maintain documentation as proof of all training activities conducted.
5. Develop and enforce the following key Policies and Notices
   - Data Protection Policy
   - Data Retention and Deletion Policy/Schedule
   - Privacy Notice/Statement/Cookies policy
   - Any other relevant policies in compliance with the Act.
6. Data Protection Impact Assessment (DPIA)
   - MUWASCO should identify all high-risk data processing activities that may impact the rights and freedoms of data subjects and conduct a Data Protection Impact Assessment (DPIA). Particular attention should be given to the use of

biometrics, Utility Master, and RexSoft systems. Submit the same to the Office of the Data Protection Commissioner for consideration.

7. Record of Processor Contracts

   Maintain up-to-date records of contractual agreements between MUWASCO and all its processors (e.g., Wonderkid Multimedia, REXSOFT, Trident, Superior Smart Security Ltd, and any other Processor or third parties MUWASCO is engaging with).

   - Ensure all contracts comply with the Data Protection Act and its regulations.

8. Data Sharing Agreements
   - Ensure that all data sharing agreements are in place and comply with applicable legal requirements.
9. Data Protection by Design and by Default
   - Produce documentation that demonstrates how Utility Master and REXSOFT applications incorporate data protection measures (Data Protection by Design and by Default) throughout their development lifecycle.
   - Include all technical and organizational measures used to protect data subjects' Privacy.
10. Mechanisms for Data Subject Rights
    - Establish/implement and document effective mechanisms that allow data subjects to exercise their rights as stipulated by the Data Protection Act.
11. Vendor management Register
    - And they keep a vendor management register to track all third parties with whom they share personal data.
12. Disaster Recovery and Backup
    - They develop a Contingency Plan, Disaster Recovery Procedures, and an incident response framework.
13. Data Protection Periodic Audits
    - They undertake periodic data protection audits to evaluate the effectiveness of their practices and ensure ongoing compliance

3 SCOPE & OBJECTIVES

The Office of the Data Protection Commissioner (the Office) is a Government agency established under the Data Protection Act, 2019 (the Act), to uphold the privacy and security of personal data. The Office enforces data protection laws and regulations and safeguards individuals' privacy and fundamental rights. The Office's mandate includes overseeing the implementation and enforcement of the Data Protection Act and its attendant regulations, which govern the processing of personal data belonging to persons located in Kenya by both public and private sector organisations.

Pursuant to Section 23 of the Data Protection Act and Regulation 53 of the Data Protection (General) Regulations, 2021, the Office must perform compliance audits and periodic inspections of data controllers and processors to ensure adherence to the Act.

Accordingly, the Office notified MUWASCO on 11th September, 2024, referencing ODPC/DPC/11/1/7, advising the organization of an in-person inspection. A follow-up reminder was dispatched on 3rd March, 2025, requesting the organisation to propose a suitable date for the inspection from 10th to 29th March, 2025. In response, MUWASCO confirmed its availability for a comprehensive audit scheduled for the 25th, 26th, and 27th of March 2025.

As agreed, the audit was carried out over three days, from March 25th to 27th, 2025, at the premises of Murang'a Water and Sanitation Company Limited in Murang'a Town. The process included interviews, observations, site visits, and reviewing the company's policies and procedures. Additionally, the Office conducted interviews with key personnel.

The Audit scope included: -

The audit encompassed a systematic sampling of processing activities across multiple departments within MUWASCO.

The Scope included -

1. Data protection governance and accountability
2. Staff data protection training and awareness

3. Security of personal data
4. Individual right requests
5. Record management
6. Data Protection Impact Assessment (DPIA) and Information Risk Management

Audit criteria included: -

1. The Data Protection Act, 2019
2. The Data Protection (General) Regulations, 2021
3. The Data Protection (registration of Data Controllers and Data Processors) regulations, 2021
4. Internal compliance documentation (Relevant policies and procedures)

4 Audit Methodology

The auditors conducted a data protection audit using a combination of the following techniques:

1) **Interviews** – Staff members involved in data processing were interviewed. The selected individuals represented the area under audit.
2) **Review of Documentation** – Relevant documents and records for each audited process were examined to assess compliance.
3) **Observation** – Inspecting data processing areas was conducted to observe practices firsthand.

The audit methods were based on sampling, meaning that some audited areas may contain additional instances of non-compliance. However, following a top-down approach, the samples were carefully selected to represent the audited areas. Priority was given to high-risk areas to enhance the audit's assurance and completeness.

Compliance Rating

The compliance rating for each scope area was categorized into three levels: C, IP, & NC.

Status Key	Meaning in Relation to DPA	Key
C	Compliant	Adequate compliance with data protection obligations
IP	In progress	Progressively taking steps to meet compliance obligations
NC	Not Compliant	No actions taken

Overall Opinion

During the audit, it was established that Murang'a Water and Sanitation Company Limited (MUWASCO) partially complies with the relevant data protection requirements. The audit report, therefore, identifies specific areas where compliance gaps exist and provides detailed recommendations for each flagged issue, aimed at helping the institution achieve full compliance and strengthen its data protection practices.

5 Audit Findings

5.1 Data Protection Governance & Accountability

Status	Observation
IP	**DATA HANDLER REGISTRATION** ▪ In accordance with Section 18 of the Data Protection Act, 2019, data controllers and processors must register with the Office of the Data Protection Commissioner (ODPC). As of this audit, MUWASCO has not fulfilled this statutory obligation and remains unregistered with the ODPC despite actively processing personal data. This non-compliance exposes the organization to regulatory sanctions and indicates a foundational data protection governance gap. ▪ MUWASCO should initiate the registration process with the Office of the Data Protection Commissioner (ODPC) as a data controller, in line with the requirements of Section 18 of the Data Protection Act, 2019. Registration is a fundamental compliance step that affirms the organization's accountability in processing personal data and reduces the risk of regulatory penalties. **Designation of the Data Protection Officer (DPO).** ▪ Pursuant to Section 24 of the Act, MUWASCO has designated a Data Protection Officer (DPO), who concurrently serves as the head of the ICT department. Additionally, departmental heads have been appointed as data protection champions. However, MUWASCO has not complied with Section 24(6) of the Act, which mandates the publication of the DPO's contact details on the institution's website and formal notification to the ODPC. Moreover, the DPO has not been issued a formal appointment letter, resulting in ambiguity regarding their official mandate, scope of authority, and functional responsibilities.

- To ensure full compliance with the Data Protection Act, 2019, the auditors recommend the following corrective actions:

  a) **Formal appointment of the DPO**

  MUWASCO should issue an official appointment letter to the DPO, clearly defining their roles, responsibilities, and reporting structure. Per data protection best practices, the appointment must ensure no conflict of interest with the DPO's other duties.

  b) **Organisational placement**

  The DPO must report directly to the highest management level and be provided with sufficient resources, autonomy, and authority to oversee the organization's data protection framework and ensure compliance with applicable legal obligations.

  c) **Qualification and competence**

  The designated DPO should possess the requisite expertise, knowledge of data protection laws, and capacity to perform the duties outlined under Section 24(7) of the Act, including cooperation with the ODPC and other relevant supervisory authorities.

  d) **Public disclosure and notification**

  In line with Section 24(6), MUWASCO must publish the DPO's contact information on its official website and formally notify the ODPC.

  e) **Operational readiness**

  MUWASCO should establish and document robust internal procedures and policies to handle data subject rights requests, such as access, rectification, erasure, and objection, ensuring timely and effective responses in line with the DPA and its regulations.

LAWFUL BASIS

Under Section 30 of the Data Protection Act, 2019, and Regulation 5 of the Data Protection (General) Regulations, data controllers must establish a lawful basis for each personal data processing activity. During staff interviews, it was observed that while MUWASCO can identify its data processing activities, it has not comprehensively mapped them to their corresponding lawful bases.

- MUWASCO's current Data Protection Policy does not explicitly specify the lawful bases for processing personal data. However, interviews with departmental heads from Admissions, Human Resources, and Procurement revealed that these individuals understand the lawful bases applicable within their functions and can articulate how they ensure compliance in practice.

- MUWASCO must update its Data Protection Policy to explicitly identify and document the lawful bases relied upon for all personal data processing activities, which must be in line with statutory requirements. The organization should also maintain internal records demonstrating compliance with these lawful bases, including procedural and technical controls.
- Additionally, MUWASCO should implement targeted training programs to ensure all employees, particularly those involved in data handling, are fully aware of the lawful bases underpinning data processing within the organization and understand their obligations for compliance.
- MUWASCO must reinforce organisational accountability by ensuring all processing activities are strictly aligned with its stated

purposes, as required under Section 30 of the Act. Any deviation from the specified purpose without a lawful basis constitutes a contravention and may attract legal and regulatory consequences.

CONSENT

The audit revealed that MUWASCO does not have a Data Protection Policy or a Privacy Statement, which are essential requirements under the Data Protection Act 2019. According to Section 25 of the Act, data controllers and processors must handle personal data legally, reasonably, and transparently. Section 41 requires appropriate technical and organizational safeguards to uphold data protection principles.

Section 30(1)(a) stipulates that data subjects must be informed about the purpose and legal basis for processing their personal data, typically achieved through a Privacy Statement. The absence of these key documents at MUWASCO compromises transparency and leaves data subjects unaware of how their personal data is collected, used, or protected.

To meet the Act's requirements, MUWASCO must urgently develop and adopt a comprehensive Data Protection Policy and ensure that Privacy Statements are publicly accessible. This will promote transparency, accountability, and adherence to the law.

INCIDENCE REPORTS AND RESPONSE

The audit established that MUWASCO lacks a formal Incident Response Plan (IRP) and the necessary mechanisms for managing personal data breaches, which pose significant legal, operational, and reputational risks under the Data Protection Act, 2019 (DPA 2019).

Pursuant to Section 43, data controllers must notify the Office of the Data Protection Commissioner (ODPC) of any personal data breach within 72 hours, while data processors must notify controllers within 48 hours of becoming aware. Non-compliance may result in sanctions under Section 63.

To meet statutory obligations and uphold accountability, the auditors recommend that MUWASCO must:

a) Develop and implement a formal IRP with defined roles, escalation paths, and notification procedures to ODPC and affected data subjects.
b) Maintain a Data Breach Incident Register documenting all incidents.
c) Establish breach notification policies and SOPs detailing severity assessments, documentation protocols, and communication workflows.
d) Review and update breach response documentation to reflect evolving legal and threat landscapes.

Failure to establish these controls undermines MUWASCO's compliance posture and elevates the risk of delayed, inadequate, or unreported data breach responses.

POLICIES IN PLACE

The audit established that MUWASCO has only two formally adopted policy documents: the ICT Policy and the Human Resource Policy and Procedure Manual. While a Data Protection Policy is reportedly under development, it remains in draft form and has not yet been finalized, approved, or operationalized.

	Critical gaps were identified in the organisation's policy framework, specifically about personal data governance, regulatory compliance, and information security. The absence of the following essential policies constitutes a material non-compliance with the Data Protection Act, 2019, and related best practice standards. The auditors recommend that MUWASCO finalize the policies currently in draft form and develop the remaining ones, i.e. i. Data protection policy (draft) ii. Data retention and deletion policy and schedule iii. Data breach response plan and disaster recovery plan (draft) iv. Privacy notice v. Cookies policy vi. Email policy The absence of these foundational governance documents represents a significant compliance deficiency and operational risk. Immediate action is recommended to develop, approve, and implement the missing policies and integrate them into the broader data protection and information governance framework. The policies must be aligned with the data protection principles outlined in Section 25 of the Act.

5.2 Staff Data Protection Training & Awareness

Status	Observation
NC	The audit findings indicate a critical skills and awareness gap among personnel at MUWASCO regarding data protection and cybersecurity. This deficiency constitutes a substantial compliance and operational risk under the Data Protection Act, 2019 (DPA), particularly for the principles

of data minimization, purpose limitation, lawfulness of processing, and security safeguards as outlined under Part IV of the Act.

Several employees demonstrated limited familiarity with foundational data protection concepts, including, but not limited to, data subject rights, lawful bases for processing, and organizational obligations for data security and breach notification. This lack of awareness increases the likelihood of inadvertent breaches, improper data handling, and regulatory non-compliance.

Although MUWASCO conducted its last formal data protection training on 13th December 2023, the audit revealed no evidence of a structured or continuous training program. Furthermore, there is no indication that the training was role-based or aligned with the varying responsibilities of staff members who routinely handle personal or sensitive data. Under Section 25(c) and Section 41 of the DPA, data controllers and processors must ensure that appropriate technical and organizational measures are in place, including training, to ensure compliance and uphold the rights of data subjects. The absence of ongoing capacity building and awareness programs compromises accountability and data security readiness.

To remediate these gaps, the auditors issued the following directives:

- **Design and implementation of training programs**
  Create standardized, legally compliant training content aligned with data protection and cybersecurity best practices. Implement a mandatory training schedule covering privacy, incident response, and secure data handling.
- **Assessment and validation**

	Introduce pre-/post-training evaluations and scenario-based assessments to ensure retention and applicability. ▪ **Monitoring and improvement** Track participation, performance, and refresher needs, and regularly update training content. The audit also found that critical departments (Security, Customer Services, Finance and Accounts, HR, Supply Chain) lack formal policies and SOPs governing data access and handling. The auditors further directed that MUWASCO must: • Sensitize departmental heads on the Data Protection Act. • Deliver targeted, role-based training for staff handling personal data. • Develop and enforce department-specific SOPs for data governance. Implementing a structured, ongoing training and policy framework will improve compliance, reduce operational risk, and enhance MUWASCO's capacity to protect personal data and digital infrastructure.

5.3 Security Of Personal Data

Status	Observation
NC	**DATA SECURITY** The audit established that MUWASCO has implemented a CCTV surveillance system across various operational zones to support security and asset protection objectives. While such surveillance may be justified under the lawful basis of legitimate interests pursuant to Section 30 of the Data Protection Act, 2019, specific deployments were found to pose potential infringements on data subject rights.

Specifically, two CCTV cameras were observed to be installed within internal working areas where employees perform routine tasks. The continuous monitoring of these spaces raises serious concerns regarding the proportionality and necessity of surveillance, potentially breaching the data minimization and purpose limitation principles outlined in Section 25 of the Act unless justified and supported by a Data Protection Impact Assessment (DPIA), surveillance of employees in their workspaces may amount to excessive and unlawful processing of personal data.

One CCTV camera was also noted to capture footage beyond MUWASCO's premises, including adjacent residential or public areas. This constitutes extraneous monitoring, which exceeds the organisation's lawful surveillance mandate and may infringe on the privacy rights of third-party data subjects not affiliated with MUWASCO. Such a configuration must be reviewed and re-aligned to ensure that footage capture is confined strictly to areas under MUWASCO's legal or operational control.

The auditors advise MUWASCO to:

a) Reassess the positioning of all CCTV installations and ensure alignment with the necessity and proportionality criteria established under the Act.
b) Immediately conduct a DPIA for all surveillance operations, in line with Section 31 of the Act and Regulation 49 of the Data Protection (General) Regulations.
c) Reconfigure or turn off CCTV units that capture workspaces or external environments without sufficient legal or operational justification.

d) Implement appropriate privacy notices in monitored areas and ensure data subjects are informed of the purpose, scope, retention periods, and rights related to CCTV surveillance.
e) Apply strict technical and organizational controls for access to recorded footage, including role-based access, encryption, and secure deletion protocols.

The audit confirmed that MUWASCO utilizes a document shredder to destroy waste paper records. This represents a compliant physical security control aligned with the storage limitation, integrity, and confidentiality principles under Sections 25 and 41 of the Act. MUWASCO is encouraged to integrate this practice into a formalized data retention and disposal policy governing physical and electronic records.

Further, the audit identified critical security gaps and widespread non-conformities within MUWASCO's technical and organizational security framework. These findings indicate a significant deviation from the obligations imposed under Section 41 of the Act and associated regulatory requirements.

The specific deficiencies observed are as follows:

Lack of core data protection and security governance policies

MUWASCO lacks formally adopted and enforced policies for establishing baseline data protection and security controls. The policies lacking in place include:

a) Password management policy
b) Bring Your Own Device (BYOD) policy
c) Email and acceptable use policy
d) CCTV surveillance policy
e) Data retention policy

f) Cookie policy

g) Privacy notice

The lack of these essential governance documents results in undefined security expectations, weak end-user accountability, and provides inadequate legal justification for processing personal data, thereby violating Sections 25 and 41 of the Act.

Inadequate physical key management practices

The audit revealed the absence of a formalized Physical Key Management Policy governing the issuance, tracking, use, and revocation of physical office keys. The lack of structured controls over physical access mechanisms exposes MUWASCO to heightened risks of unauthorized entry, tampering, and unregulated access to areas where personal data may be stored or processed.

Lack of structured and periodic staff training

MUWASCO does not conduct regular cybersecurity, data protection awareness, or training. This results in poor security hygiene, user-related vulnerabilities, and organisational non-compliance with Section 41 of the Act, which mandates training on secure personal data handling practices.

Use of legacy and unsupported operating systems

Endpoints running Windows 7, an end-of-life operating system, remain active. Microsoft no longer supports these devices and cannot receive critical security patches, violating security-by-design and security-by-default principles outlined in Section 41(1) of the Act and related technical guidelines.

Flat network architecture and lack of network segmentation

MUWASCO employs a flat network topology without segmentation between operational, user, and administrative domains. Additionally, no centralized wireless LAN controller is in place, exposing the entire network to lateral movement, unauthorized access, and inadequate control over wireless endpoints.

Inappropriate physical access to sensitive infrastructure

The audit established that the designated data center environment has been repurposed as a general working area, effectively dissolving its status as a restricted, controlled-access facility. Additionally, removing the biometric access control mechanism further weakens physical security controls, exposing the infrastructure to heightened risks of unauthorized access, data compromise, and insider threats. This configuration contravenes the confidentiality and integrity requirements under Section 25(f) of the Data Protection Act, 2019. The absence of strong physical access restrictions in areas housing critical systems and data assets significantly undermines the organizational obligation to implement appropriate technical and organizational measures under Section 41 of the Act.

Improper credential management and shared account usage

Multiple users were found to:

a) Share login credentials and passwords for enterprise systems.
b) Store sensitive system credentials (e.g., for the Utility Master application) in unencrypted browser autofill features.

These practices are inconsistent with fundamental IAM principles, violate non-repudiation and user accountability requirements, and create significant attack surfaces for credential theft and unauthorized access.

Privilege mismanagement and absence of Role-Based Access Control (RBAC)

It was observed that users from different departments were granted identical access rights within the Utility Master platform, without role-based provisioning. This violates the least privilege (PoLP) principle and purpose limitation.

The auditors directed MUWASCO to:

a) Develop, formalize, and enforce core information security policies aligned with the Data Protection Act.

b) Establish and enforce a comprehensive physical key management framework that incorporates key issuance and return logs, role-based key assignment, incident reporting for lost or stolen keys, periodic key inventory audits, and procedures for re-keying and decommissioning access upon staff exits or role changes.

c) Design and operationalize a mandatory, recurring data protection and cybersecurity training program for all staff.

d) Migrate all legacy systems to supported, patched operating environments, and maintain continuous vulnerability management.

e) Redesign network infrastructure to implement logical segmentation, VLANs, access control lists (ACLs), and deploy centralized wireless management.

f) Restrict physical access to the data center, enforce surveillance and access logs, and integrate access controls with identity verification.

g) Eliminate shared user accounts, enforce unique authentication, and deploy enterprise credential management tools with encryption and audit logging.

	h) Implement a robust RBAC framework within the Utility Master Application and other critical systems, aligning access rights with organizational roles, job functions, and data sensitivity.

5.4 Individual Rights Request

Status	Observation
NC	**Data Subject Rights** Sections 26 and 38 of the Act require data controllers to provide data subjects with precise, accessible mechanisms to exercise their rights, including the right of access, rectification, objection, and data portability. While the auditors noted that MUWASCO has developed forms intended to support these rights, it remains non-compliant with the Act due to the absence of documented procedures that outline how data subjects can submit such requests. These forms are not readily available through public channels like the organisation's website or customer service desks. This lack of accessibility and procedural clarity hinders data subjects' ability to exercise their rights and reflects a gap in MUWASCO's compliance with the statutory obligations. To best comply with Sections 26 and 38 of the Act, the auditors recommend that MUWASCO should: **Develop clear, accessible forms** Create standardized forms for all data subject rights (e.g., access, correction, erasure, objection, data portability). **Publish forms online** Make the forms easily accessible on the organisation's website.

Provide forms at all customer interaction points

Ensure physical copies are available at customer care desks or service centers.

Include guidance

Accompany forms with plain-language instructions on how to fill them out and submit requests, including timelines for response.

Designate a contact point

Provide the contact details of the Data Protection Officer (DPO) or relevant staff responsible for handling requests.

Ensure accessibility

Ensure the forms are accessible to people with disabilities, such as by providing screen reader-friendly versions or Braille copies where needed.

Maintain records

In compliance with accountability obligations, maintain a detailed log of all data subject requests and the actions taken in response.

CONSENT MECHANISMS

The audit revealed that MUWASCO does not have a Data Protection Policy or a Privacy Statement, which are essential requirements under the Act. According to Section 25 of the Act, data controllers and processors must handle personal data legally, fairly, and transparently. Section 41 requires appropriate technical and organizational safeguards to uphold data protection principles.

In addition, Section 30(1)(a) stipulates that data subjects must be informed about the purpose and legal basis for processing their personal data, typically achieved through a Privacy Statement. The absence of these key documents at MUWASCO compromises transparency and leaves data subjects unaware of how their personal data is collected, used, or protected.

	To meet the requirements of the Act, MUWASCO must urgently develop and adopt a comprehensive Data Protection Policy and ensure that Privacy Statements are publicly accessible. This will promote transparency, accountability, and adherence to the law.

5.5 Records Management - Details of Processing Activities

Status	Observation
NC	**RECORDS OF PROCESSING ACTIVITIES (RoPA)** MUWASCO demonstrates partial compliance with data protection obligations by maintaining the capability to identify the categories of data subjects and the corresponding categories of personal data collected. Data subjects include employees, customers (and their dependents), and third-party entities such as suppliers or vendors. This classification forms the basis for understanding processing scope and mapping data flows within the organization. MUWASCO lacks a formal Record of Processing Activities (ROPA), although not expressly required under the Act, maintaining a RoPA is consistent with internationally recognized best practices in data governance. An accurate and current RoPA is fundamental to implementing key data protection principles, including purpose limitation, data minimization, and accountability. It provides a structured mechanism for documenting and categorizing personal data processing operations, detailing data subject categories, types of personal data processed, and the lawful bases for processing. This documentation framework strengthens an organization's capacity to evaluate, oversee, and reduce data protection risks throughout the entire data processing

lifecycle. Immediate remediation is required through the development of a comprehensive ROPA document. This record must outline:

a) The nature and purpose of all processing activities;
b) The lawful basis applicable to each processing operation;
c) The categories of personal data processed;
d) The categories of data subjects involved;
e) The identity of third-party recipients or processors; and
f) The sources from which personal data is collected.

The ROPA should also be continuously updated and integrated with internal governance controls to ensure sustained compliance and auditability.

Categories of data subjects and personal data

The organization processes data across several subject classes:

Employees: Personal data collected includes full names, national ID copies, National Social Security Fund (NSSF) details, bank account information, photographs, information about dependents, religion (as required by the National Employment Authority), gender, age, ethnicity, and academic qualifications.

Customers and their dependents: Data collected comprises names, contact numbers, email addresses, property identification details (such as plot numbers and title deeds), Kenya Revenue Authority (KRA) Personal Identification Numbers (PINs), and national ID numbers.

Third-party vendors and suppliers: These may include service providers involved in payroll, client management, insurance, and physical security operations.

Data collection and processing systems

Customer data is collected primarily through a customer relationship management system called UTILITY Master, developed and maintained by Wonderkid Multimedia. Payroll-related data is managed using the REXSOFT accounting system, which is hosted internally within the organisation. All personal data is collected directly from the data subjects during onboarding or operational engagements, ensuring a traceable and consent-driven acquisition process.

Third-party data processors

The organization engages several external entities in the processing of personal data:

a) Utility Master by Wonderkid Multimedia – Client data management system
b) REXSOFT – Payroll and human resource accounting system
c) Trident – Insurance service provider
d) Superior Smart Security Ltd – Physical security services provider

These third-party processors must be subjected to due diligence, including data protection impact assessments and the establishment of data processing agreements (DPAs), to ensure compliance with contractual and statutory data protection requirements.

DATA RETENTION AND DELETION /SCHEDULE

The auditors established that Murang'a Water and Sanitation Company Limited (MUWASCO) does not have a formally documented Data Retention Policy, a critical deficiency in the context of compliance with the Data Protection Act, 2019. The absence of such a policy constitutes a breach of Section 41, which obligates data controllers and data processors to implement appropriate technical and organizational

	safeguards to ensure data security, including mechanisms for the retention and secure disposal of personal data. The Act stipulates that personal data shall not be retained for longer than is necessary to fulfil the purpose for which it was collected. This provision codifies the data protection principles of storage limitation and purpose limitation. The audit observed that MUWASCO's enterprise applications and data processing systems lack embedded data lifecycle governance features despite these statutory requirements. Specifically, there is no defined data retention framework, retention schedule, or workflow for data disposal. The systems do not offer a mechanism through which data subjects can ascertain the duration for which their personal data is retained, nor initiate erasure requests. To align with the Data Protection Act, 2019 and associated best practices, the auditors direct MUWASCO to develop and adopt a comprehensive Data Retention and Disposal Policy, articulating governance principles, retention criteria, and procedural controls for the lifecycle management of personal data.

5.6 Data Protection Impact Assessment (DPIA)

Status	Observation
NC	Section 31 of the Data Protection Act, 2019 (hereinafter "the Act"), imposes a mandatory obligation on data controllers and data processors to conduct a Data Protection Impact Assessment (DPIA) where a processing operation is likely to result in a high risk to the rights and freedoms of data subjects. This assessment must be conducted at least sixty (60) days before the commencement of such processing. Regulation 49 of the Data Protection (General) Regulations enumerates

specific categories of processing operations presumed to present a high risk, including but not limited to large-scale processing of sensitive personal data, surveillance activities, and use of biometric data for uniquely identifying individuals.

The audit established that MUWASCO operates three principal systems for core business functions:

a) UTILITY Master – A client management system developed and hosted by Wonderkid Multimedia.
b) REXSOFT – A payroll management system.
c) Biometric Access System – Used to log employee entry and exit times.

Despite operationalizing these systems, MUWASCO has not conducted any DPIAs in accordance with Section 31(2) of the Act. Notably, the use of biometric data and other intrusive technologies, particularly those involving automated decision-making or monitoring of employees, inherently introduces a high risk to the rights and freedoms of data subjects. As such, these processing operations fall squarely within the scope of Regulation 49 and warrant the execution of DPIAs.

MUWASCO is therefore advised to:

1) Refer to Regulation 49 of the General Regulations to identify processing operations that require a DPIA.
2) Immediately undertake DPIAs for all relevant systems in line with Section 31(2) of the Act and the published Guidance Note on Data Protection Impact Assessments.
3) Involve the designated Data Protection Officer (DPO) in all stages of the DPIA process as mandated by best practice and regulatory guidance

	Each DPIA must contain the following elements: a) A systematic description of the envisaged processing operations and their purposes. b) An assessment of the necessity and proportionality of the processing concerning those purposes. c) A risk assessment evaluating the potential impact on the rights and freedoms of data subjects, particularly concerning data minimization, storage limitation, and profiling. d) A detailed description of technical and organisational measures proposed to mitigate identified risks, including data security controls, access management, and anonymization or pseudonymization where applicable. MUWASCO must implement a formal risk-monitoring mechanism capable of detecting changes in the risk landscape associated with its processing activities. This mechanism should include procedures for revising DPIAs in light of new threats, evolving technologies, or changes in data processing practices. Where risks cannot be adequately mitigated, MUWASCO must document the rationale and seek prior consultation with the Office of the Data Protection Commissioner (ODPC) as per Section 31(3) of the Act.

5.7 Data Sharing

Status	Observation
NC	In line with Section 30 of the Act, and the Data Protection (General) Regulations, 2021, MUWASCO shares personal data with third parties such as the National Environment Authority (NEA), Trident (an insurance firm), the National Social Security Fund (NSSF), and the Kenya Revenue Authority (KRA), as required by its operational needs and legal obligations. A valid legal basis must support this kind of data sharing,

	typically a legal obligation or a contractual necessity. It must follow the principles of data minimization, purpose limitation, and accountability. Under Section 41 of the Act, MUWASCO must also implement appropriate technical and organizational measures to protect personal data during transfer and processing and maintain comprehensive Records of Processing Activities (ROPA) to demonstrate compliance. To ensure transparency and uphold data subjects' rights, MUWASCO must communicate how personal data is used, for what purpose, and with whom it is shared. This is typically done through a privacy statement, which helps inform individuals and reinforces MUWASCO's commitment to lawful and responsible data handling.

5.8 Vendor Management

Status	Observation
NC	In accordance with Section 41 of the Data Protection Act, 2019, which requires data controllers and processors to implement appropriate technical and organisational measures to safeguard personal data, the audit identified a critical gap in Murang'a Water and Sanitation Company Limited's (MUWASCO) IT governance framework specifically, the absence of a formal Vendor Management System (VMS). The auditors also found that many core infrastructure components, including enterprise applications, user endpoint devices, network switches, and wireless access points, ran on end-of-life (EOL) firmware or unsupported operating systems. This presents a significant information security risk. EOL systems no longer receive security updates, firmware patches, or vendor support, exposing them to known vulnerabilities such as privilege escalation, remote code execution (RCE), and denial-of-service (DoS) attacks.

	These weaknesses increase the likelihood of unauthorized access, data breaches, and operational disruptions, placing both company systems and personal data at risk.

5.9 Implementation of Privacy by Default AND Design

Status	Observation
NC	Pursuant to Section 41 of the Act, and Regulations 27 to 36 of the Data Protection (General) Regulations, data controllers and processors are obligated to implement appropriate technical and organizational measures to ensure the security and integrity of personal data. The principle of privacy by design mandates the proactive integration of data protection principles, as set out under Section 25 of the Act, into the architecture of information systems, business processes, and service delivery models. This approach embeds data privacy safeguards at the foundational level of system and process development, ensuring compliance is not retrofitted but inherent to the design and operation of organisational functions. MUWASCO should ensure that the principles of privacy by design and privacy by default are systematically embedded within the organization's governance framework and integrated throughout the entire project and system development lifecycle. The organization must be capable of demonstrating, through documented policies, procedures, and technical controls, how it operationalizes and ensures ongoing compliance with the data protection principles outlined in Section 25 of the Act. This includes evidence of proactive measures to embed data protection into business practices, risk assessments, and decision-making processes from inception through implementation.

6 RESTRICTIONS AND LIMITATIONS

MUWASCO gave the auditors access to all necessary information, documentation, and personnel to conduct the assessment effectively. MUWASCO also demonstrated full cooperation throughout the process, ensuring the auditors had the support and resources needed for a comprehensive evaluation.

7 RECOMMENDATIONS

The auditors recommend:

1. That MUWASCO should immediately initiate the registration process with the Office of the Data Protection Commissioner (ODPC) as a data controller and processor.
2. That MUWASCO formally appoints a Data Protection Officer (DPO) and issues an official letter that outlines clear roles and responsibilities with no conflict of interest. And that the DPO's contact information be published on MUWASCO's official website and submitted to the Office of the Data Protection Commissioner,
3. That MUWASCO should undertake comprehensive data mapping across all departments to document the types of personal data processed, describe each category, and identify the lawful basis for collection,
4. That they implement structured data protection and cybersecurity training programs for staff,
5. That they develop and enforce critical policies and notices, including but not limited to Data Protection Policy, Data Retention and Deletion Policy, Privacy Notice,
6. That they undertake a Data Protection Impact Assessment (DPIA) on processing operation that are likely to result in high risk to the rights and freedoms of a data subject, by virtue of its nature, scope, context and purpose,
7. That they maintain a record of all third parties MUWASCO is engaging with and that they ensure that the contracts between them and the third parties are in compliant with the Act,
8. That MUWASCO should be in a position to demonstrate how they have incorporated data protection by design or by default on all their systems and

applications used by the organisation. And that they document all the technical and organizational safeguards they have incorporated into the systems/Applications without relying on the external developers to demonstrate on their behalf,

9. They put in place mechanisms to allow data subjects to exercise their rights
10. And they keep a vendor management register to track all third parties they share the persona data with,
11. That they develop a Contingency Plan, Disaster Recovery Procedures, and an incident response framework,
12. That they undertake periodic data protection audits to evaluate the effectiveness of its practices and ensure ongoing compliance.

8 ANNEXURE 1: MANAGEMENT RESPONSE

We have identified short-term, medium term and long-term actions that MUWASCO should address to strengthen its data protection practices and ensure compliance.

NO	FINDING SUMMARY	DESCRIPTION	CRITERIA	RECOMMENDATION	MANAGEMENT RESPONSE	DURATION
1	The organisation lacks a comprehensive Record of Processing Activities (RoPA).	MUWASCO has failed to outline its processing activities and establish the lawful basis relied upon, resulting in the absence of clearly documented processing purposes, data categories, data flows, and corresponding legal justifications—ultimately hindering accountability and transparency in its data processing operations	Section 30 of the Act and Regulation 5(2) in the General Regulations	It is essential to conduct a comprehensive data mapping exercise to identify all processing activities, delineate the categories of personal data collected, specify the intended purposes for each processing operation, and establish the corresponding lawful basis in accordance with the Data Protection Act, 2019.		
2	There is no tangible evidence of implementing privacy by design or	Through documented policies, procedures, or technical controls, there was no evidence of how MUWASCO operationalizes and maintains ongoing	Sections 25 and 41 of the DPA and regulations 27-36.	Develop comprehensive technical documentation for Utility Master and RexSoft, including: a detailed user requirements analysis, system		

	default principles.	compliance with the data protection principles set out in Section 25 of the Data Protection Act, 2019. This includes the absence of proactive measures to integrate data protection into business practices, conduct risk assessments, and incorporate privacy considerations into decision-making from the outset through to implementation		architecture and functional specifications, expert technical evaluation reports, standardized test checklists for system validation, audit log frameworks for traceability and accountability, and formalized third-party service level and data processing agreements.		
3	No data protection impact assessments have been carried out.	MUWASCO has not conducted any Data Protection Impact Assessments (DPIAs). The use of biometric data and other intrusive technologies, especially those involving automated decision-making	Section 31(2) of the DPA	MUWASCO should identify all high-risk data processing activities that may impact the rights and freedoms of data subjects and conduct a Data Protection Impact Assessment (DPIA).		

		or employee monitoring, presents a high risk to the rights and freedoms of data subjects.		Particular attention should be given to the use of biometrics, Utility Master, and RexSoft systems		
4	Murang'a Water and Sanitation Company Limited lacks key policies pivotal in Data protection and cookie policy.	MUWASCO lacks essential policies, including password and email policies, which increases the organization's exposure to data security risks, cyber threats, and unauthorized access to information. Additionally, the absence of a cookie policy prevents users from providing informed consent for cookie use and leaves them unaware of data tracking practices.	Section 25, 30(1)(a) and 32 of the DPA	MUWASCO should mandate official organizational email, establish comprehensive network and CCTV management policies, and conduct regular system management audits. Additionally, a cookie policy pop-up should be implemented on the website's landing page to enable users to review, manage, and provide informed consent for specific categories of cookies before storage		

5	There is no data retention and erasure policy	There is no clear guideline on the retention and erasure of data.	Section 39(1), section 41 of the DPA	Develop a comprehensive data protection policy and schedule to ensure transparency, accountability and compliance with the act.		
6	Lack of a vendor management system	MUWASCO's critical devices are running on end-of-life firmware, posing a significant security vulnerability.		Establish a structured vendor management framework and upgrade all legacy devices to ensure they operate on the latest vendor-supported firmware.		
7	There is no training program for data protection	The majority of employees have not yet received sufficient training on data protection	Section 41	Implement mandatory staff training on data protection and cybersecurity		
8	Lack of an incident reporting and	This absence exposes MUWASCO to delayed threat detection, ineffective incident containment, and an	Section 43 (1)	Develop and implement an incident reporting framework to ensure compliance.		

	response framework.	increased risk of data breaches, unauthorized access, and regulatory non-compliance.				
9	Lack of data protection policy and privacy statement	This absence indicates a lack of transparency, leaving a grey area on the collection, processing and protection of personal data.	Section 25 of the DPA Section 30(1) (a)	Develop and implement an elaborate data protection policy and publicly accessible privacy statements		

For: DATA PROTECTION COMMISSIONER
P. O. Box 30920-00100,
NAIROBI