



Kenya Power

THE KENYA POWER & LIGHTING COMPANY PLC

DATA PROTECTION POLICY

Part A - Document Control Sheet			
Document	Data Protection Policy		
Document Owner	Manager, Board & Regulatory Affairs		
Division	Legal, Regulatory Affairs & Company Secretary		
Department	Board & Regulatory Affairs		
Lead Contact	Manager, Board & Regulatory Affairs		
Document Status	Final		
Document Approvals	Approver	Approval Reference	Approval Date
	Executive Committee	EXCOM/389/23	Mon. 20 th Nov. 2023
	Board of Directors	BM/164/23	Mon. 4 th Dec. 2023
Reference. No.	KPLC1/2B/5/1/015		
Issue No.	01		
Revision No.	Not Applicable		
Revision Date	None		
Revision Type	Not Applicable		
First Development Date	Friday, 1 st September 2023		
Commencement Date	24 TH JUNE 2024		
Revision Frequency	Three (3) Years		
Next Review Date	June 2027		
Superseded Documents	None		
Complementary Documents	All Company Policies		

DATA PROTECTION POLICY

Part B - Definitions and Abbreviations

Anonymization	Means the removal of personal identifiers from Personal Data so that the Data Subject is no longer identifiable
Consent	Means any manifestation of express, unequivocal, free, specific and informed indication of the Data Subject's wishes by a statement or by a clear affirmative action, signifying agreement to the processing of Personal Data relating to the Data Subject
Certificate of Registration	Means a Certificate issued by the Office of the Data Protection Commissioner upon registration as a Data Controller and/or Data Processor and which shall remain valid for a period of two (2) years and renewable after expiry
Complaints Register	Means a register maintained by KPLC outlining all complaints received from Data Subjects, investigations, details of the outcome of investigations and how complaints have been addressed by KPLC
Compliance Reports	Means information and data showing KPLC's status of compliance with all legal and regulatory requirements on data protection including any Personal Data Breaches and complaints from Data Subjects
Data Controller	Means a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing of Personal Data
Data Processor	Means a natural or legal person, public authority, agency or other body that processes Personal Data on behalf of

the Data Controller

Data Subject	Means an identified or identifiable natural person who is the subject of Personal Data
Direct Marketing	Means any advertising or promotions that relies on direct communication or distribution to individual consumers through either email, social media or text campaigns rather than through a third party such as mass media
Encryption	Means the process of converting the content of any readable data using technical means into a coded form
Personal Data	Means any information relating to an identified or identifiable natural person
Personal Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed
Processing	Means any operation or sets of operations which is performed on Personal Data or on sets of Personal Data whether or not by automated means which includes: - a) collection, recording, organizing, structuring b) storage, adaptation or alteration c) retrieval, consultation or use d) disclosure by transmission, dissemination, or otherwise making available e) alignment, combination, restriction, erasure or destruction
Pseudonymisation	Means the processing of Personal Data in such a manner that the Personal Data can no longer be attributed to a specific Data Subject without the use of additional

information and such additional information is kept separately and is subject to technical and organizational measures to ensure that the Personal Data is not attributed to an identified or identifiable natural person.

Risk Register

Means a register maintained by KPLC detailing new and on-going data protection risks affecting KPLC

Regulator

Means the Office of the Data Commissioner established under the Act to regulate compliance with data protection laws and principles by Data Controllers and Data Processors and take enforcement actions in case of non-compliance

Sensitive Personal Data

Means Personal Data revealing the natural person's race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including names of the person's children, parents, spouse(s), sex or the sexual orientation of the Data Subject

Staff

Means employees of KPLC.

Third Party

Means natural or legal person, public authority, agency or other body, other than the Data Subject, Data Controller or Data Processor who, under the direct authority of the Data Controller or Data Processor, are authorized to process Personal Data

Training Program

Means a set of activities intended to create awareness and ensure compliance with the Data Protection Act, 2019 by KPLC.

Part C – Introduction

The Kenya Power & Lighting Company PLC (KPLC) collects, processes and stores Personal Data belonging to Data Subjects and acknowledges the importance of safeguarding such Personal Data. This Policy therefore establishes the framework for Processing Personal Data in accordance with the Data Protection Act, 2019 ("the Act") and the regulations thereto.

Part D – Policy Purpose and Objectives

1. Establish the required framework for Processing of Personal Data held by KPLC while proactively responding to the legal and regulatory compliance obligations stipulated under the Act.
2. Ensure effective protection and management of Personal Data by identifying, assessing, monitoring and mitigating privacy risks in any activities involving the collection, retention, use, disclosure and disposal of Personal Data by KPLC.
3. Ensure KPLC has internal controls and mechanisms in place that adequately mitigate any risks of Personal Data Breaches.
4. Ensure KPLC maintains public trust regarding the safety of the Personal Data it holds.
5. Ensure KPLC maintains a good relationship with the Regulator by complying with all legal and regulatory requirements.
6. Engender a culture of data protection and privacy across KPLC.
7. Mitigate against financial losses to KPLC arising from penalties that may be imposed as a result of Personal Data Breaches and non-compliance with applicable laws.

Part E – Policy Statements

1. **Company Obligations:** -
 - 1.1 Designate a member of Staff of the Board & Regulatory Affairs Department who shall ensure compliance with data protection laws and regulations
 - 1.2 Publish the contact details of the person handling all matters relating to

data protection on its website and communicate them to the Office of the Data Commissioner who shall ensure the same information is available on the website

- 1.3 Register as a Data Controller and Data Processor and periodically renew the registration as required. Applications for renewals to be made thirty days before expiry of the Certificate of Registration
- 1.4 Ensure that all Personal Data Breaches are reported to the Office of the Data Commissioner expeditiously within seventy-two (72) hours of becoming aware of such breaches and to the Data Subject in writing within a reasonably practical period
- 1.5 Conduct a Data Protection Impact Assessment (DPIA) with a view of identifying risks arising out of the processing of Personal Data and minimizing these risks as early as possible
- 1.6 Conduct privacy and information audit and risk assessment at each stage of every project or initiative involving collection, processing, transmitting, storage, use and disposal of Personal Data
- 1.7 Apply appropriate Personal Data security controls such as Encryption, Anonymization and Pseudonymisation of Personal Data
- 1.8 Continuously train employees on data privacy requirements and obligations of the Company
- 1.9 Submit quarterly reports to the Executive Committee on the legal and regulatory requirements of the Company including any Personal Data Breaches and the corrective actions being taken to address/reduce such breaches.

2. Principles of Data Protection

- 2.1 In processing of Personal Data, KPLC will comply with the following guiding principles: -
 - 2.1.1 **Lawfulness, Fairness and Transparency.** Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. In this regard, a Data Subject shall be sufficiently informed of the name of the Data Controller and the purpose(s) for processing their Personal Data
 - 2.1.2 **Legitimacy.** The processing of Personal Data shall have a legal and legitimate basis and shall be processed only if there is a legitimate

- purpose for the processing of such data
- 2.1.3 **Purpose Limitation.** Personal Data collected by KPLC shall only be used for the purpose that was outlined before the data was collected and shall not further be processed or used in a manner that is incompatible or inconsistent with those purposes
- 2.1.4 **Data Minimization.** Personal Data collected shall be adequate, relevant and limited to what is necessary in relation to the purpose for which the data will be processed
- 2.1.5 **Storage Limitation.** Personal data shall not be kept for longer periods than is necessary to achieve the purpose for which the data was collected and processed. Personal Data kept by KPLC shall be retained and erased as provided for in the Records Management and Records Retention Policies
- 2.1.6 **Accuracy.** Personal Data maintained by KPLC shall be accurate, complete and up to date. KPLC will take suitable steps to ensure that inaccurate or incomplete data is deleted, corrected, supplemented or updated without delay
- 2.1.7 **Integrity and Confidentiality.** KPLC shall establish suitable organizational and technical measures to prevent unauthorized access, illegal processing or distribution, as well as accidental loss, modification or destruction of Personal Data
- 2.1.8 **Transfer of Data.** KPLC shall not transfer or disclose Personal Data to a Third Party without the Data Subject's Consent and unless there is adequate proof of adequate data protection safeguards by the Third Party. The processing of Personal Data for a child shall be done only with the Consent of the child's parent or guardian
- 2.1.9 **Rights of Data Subjects.** In processing Personal Data, KPLC shall be cognizant of the following rights of Data Subjects. KPLC shall notify the Data Subject of these rights prior to processing their Personal Data: -
- a) Right to be informed of the use to which their Personal Data is to be put
 - b) Right to access of their Personal Data held by KPLC
 - c) Right to object to the processing of all or part of their Personal Data
 - d) Right to rectification if the information held is inaccurate, false, misleading or is incomplete or requires to be updated

- e) Right to complain (as would be appropriate to the Data Controller, Data Processor or Regulator)
- f) The right to object the processing of their data for Direct Marketing purposes
- g) The right to be forgotten/ the right to erasure
- h) Right to appropriate security safeguards where Personal Data is being archived for various purposes
- i) The right to appropriate security safeguards in cross border transfer of Personal Data.

Part F – Scope

This Policy applies to all Staff of KPLC especially those undertaking activities relating to processing of Personal Data belonging to Data Subjects. This Policy also sets out the requirements for the protection of Personal Data held by KPLC in manual, electronic or any other form.

Part G - Risk Statement

Misuse of Personal Data through loss, unauthorized disclosure or failure to comply with the data protection principles and the rights of Data Subjects may result in significant legal and financial damages. This may include penalties specified in the Act, litigation, regulatory sanctions and reputational damage. In order to address these risks, the Company shall put in place mechanisms and processes to mitigate against data protection risks by complying with all data protection principles and provisions of the Act.

Part H - Responsibility for Implementation of the Policy

1. **Board and Regulatory Affairs Department**
 - 1.1 Apply for registration of KPLC as a Data Controller and Data Processor and thirty days before the expiry of the Certificate of Registration, apply for renewal of the Certificate of Registration
 - 1.2 Oversee implementation and compliance with the Data Protection Act, 2019 and relevant regulations.

- 1.3 Develop, maintain and regularly update the Data Protection Risk Register.
- 1.4 Submit the relevant compliance reports to the Office of the Data Commissioner in a timely manner.
- 1.5 Oversee the conduct of a DPIA.
- 1.6 Provide Compliance Reports and status updates on the data protection and privacy obligations of KPLC to the Executive Management.
- 1.7 Conduct and advise the Company on DPIA with a view of mapping out all the data processed and held by KPLC while assessing the impact and risks of the processing activities
- 1.8 Conduct training and awareness sessions across KPLC on data privacy requirements and obligations of KPLC
- 1.9 Ensure that KPLC processes the Personal Data of its Staff, customers, service providers or any other individuals in compliance with the Act
- 1.10 Advise KPLC and employees on data processing requirements and facilitate capacity building for Staff involved in data processing operations
- 1.11 Monitor new and on-going data protection risks and update the Risk Register of KPLC
- 1.12 Support data incident management, investigations and Personal Data Breach notifications to the Office of the Data Commissioner
- 1.13 Receiving, investigating and addressing complaints from Data Subjects regarding the Personal Data held by KPLC and maintaining a Complaints Register
- 1.14 Liaise and cooperate with the Office of the Data Commissioner and any authority on matters relating to data protection while ensuring that all the risks related to data protection are captured in the register and addressed appropriately.

Part I - Monitoring and Evaluation

The Board & Regulatory Affairs Department shall oversee implementation of the provisions of this Policy.

Part J - Triggers for Policy Review

This Policy will be reviewed under the following circumstances -

1. Legal and regulatory changes
2. Change in organization structure and policies
3. Changes in the Business Environment.

Part K - Statutory and Regulatory Compliance Requirements

In the digital era data is a critical resource that drives economic growth owing to the rising amount of Personal Data being processed. As such, various data protection laws and regulations are in place with the aim of ensuring security and privacy of such data. In this regard, KPLC and Staff therein are required to comply with various laws and regulations including but not limited to: -

1. The Constitution of Kenya, 2010
2. The Data Protection Act, 2019 and the Regulations thereto including –
 - 2.1 The Data Protection (General) Regulations, 2021
 - 2.2 The Data Protection (Complaints Handling and Enforcement Procedures) Regulations, 2021
 - 2.3 The Data Protection (Registration of Data Controllers and Data Processors) Regulations, 2021
3. Relevant Legal Notices
4. Regulatory circulars, guidelines, directives and codes of practices
5. Contractual obligations regarding data protection and privacy.

Part L – Records and Reports

1. Certificate of Registration of KPLC as a Data Controller and Processor
2. Compliance Reports
3. Complaints Register
4. Records Management and Data Retention Policy
5. Risk Register
6. Training Programs.

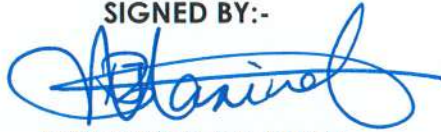
Part N - Distribution List

All Staff of KPLC to comply with the Data Protection Act, 2019 and provisions of this Policy.

Part O - Transition and Consequential Provision

The procedures giving effect to this Policy shall be developed and approved within a maximum period of six (6) months from the Commencement Date.

SIGNED BY:-



JOY BRENDA MASINDE
CHAIRMAN, BOARD OF DIRECTORS

Signature Date: 24TH JUNE 2024