



Data Protection Toolkit



***Safeguarding Data,
Upholding Trust***

Table of Content

Data Privacy Statement	Page 05
Data Sharing Guidelines	Page 19
Access Control Guidelines	Page 27
Data Breach Handling Guidelines	Page 35
Frequently Asked Questions	Page 42



Data Privacy Statement



Data Privacy Statement

1.0 Introduction

At The Kenya Power & Lighting Company PLC (“Kenya Power”), we are committed to protecting your privacy. This Privacy Statement outlines the types of personal data we collect, the reasons for collecting it, how we process it, and how you can exercise your rights regarding the use of your personal data.

This statement applies to all individuals, including customers, suppliers, contractors, and visitors to any of Kenya Power’s offices.

2.0 Definitions

References to

2.1 “You” means:

2.1.1 Customer- any individual who applies for the installation of or supply of electricity, accesses our websites, or uses any of the products and services provided by Kenya Power.

2.1.2 Any agent, supplier or contractor who has been contracted by Kenya Power, recognized as an agent under applicable laws or regulations.

2.1.3 Any visitor that is a natural person (including contractors/ subcontractors or any third parties) who gains access to any Kenya Power premises.

2.2 “Kenya Power”, “we” or “us”, “our” and “ours” means The Kenya Power & Lighting Company PLC

2.3 The word **“includes”** means that what follows is not necessarily exhaustive, and therefore, the examples given or situations are not the only ones encompassed by the meaning or explanation of the text.

2.4 Personal Data means any information that makes you identifiable as a natural person and this includes names, national identity card number, email etc.

2.5 Sensitive Personal Data includes data revealing your race, health status, ethnic social origin, conscience, belief, genetic data, biometric data, property details, marital status, family details including details of your children, parents, spouse or spouses, sex or sexual orientation.

3.0 Statement Details

3.1 Collection of Information

We collect your Personal Data with your knowledge and consent when you do any of the following (please note that this list is not exhaustive):

3.1.1 Apply for a specific product or service, including but not limited to application for installation or supply of electricity and fiber optic

3.1.2 Ask Kenya Power for more information about any of our products or services or lodge a query or complaint;

3.1.3 When you visit, access any of Kenya Power buildings/ premises or online platforms;



3.1.4 Where you have been identified as a next of kin, personal administrator by our Customer or employee;

3.1.5 Where you apply for employment at Kenya Power;

3.1.6 Make an application to Kenya Power or interact with us as an agent, supplier, consultant or contractor;

3.1.7 Respond to or participate in an event, survey etc;

3.1.8 When you make an application or engage with Kenya Power Foundation as a beneficiary;

3.1.9 We may also collect your information from other organisations including fraud prevention and government agencies;



3.2 What Information is collected?

The information we collect and store about you includes but is not limited to the following:

3.2.1 Your identity including your name, address, location, phone number, identity document type and number, date of birth, email address, and property details.

3.2.2 Your credit or debit-card information, information about your bank account numbers and SWIFT codes or other banking information.

3.2.3 Your contact with us, such as when you: call us or interact with us through email (we may record your conversations, social media or other interactions with us), register your biometric information when you visit Kenya Power premises.

3.2.4 We utilize Closed Circuit Television (CCTV) surveillance to enhance security across all Kenya Power premises. CCTV cameras



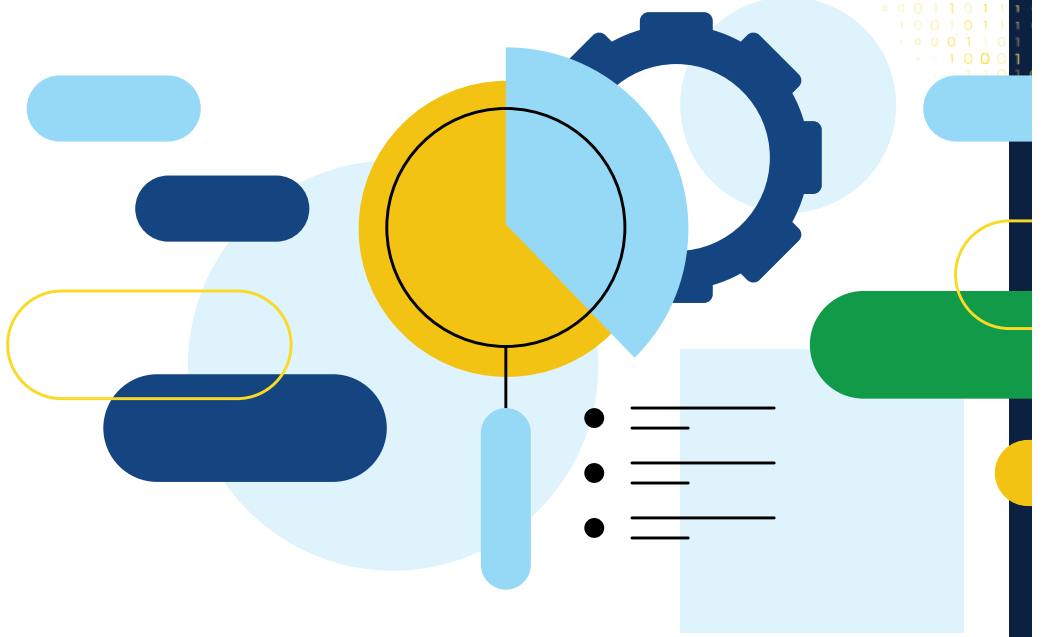
are strategically placed to ensure a safe and secure environment, supporting our commitment to safety, crime prevention, and overall security.

3.2.5 When you request a parking reservation, we collect and store your personal information (name, phone number, and vehicle registration).

3.2.6 We maintain a visitor register where we collect and store your personal information, including your name, company/institution details, phone number, vehicle registration, and National ID.

3.2.7 When you use Kenya Power WIFI for guest and visitors, we collect email IDs and will provide user name and password. We record the MAC address and also log traffic information in the form of sites visited, duration.





3.3 Use of Information

We may use and analyse your information for the following purposes:

- 3.3.1** Processing applications for the installation and supply of electricity, as well as any other products and services you may request from Kenya Power;
- 3.3.2** Collecting credit/debit card information, bank account details, and SWIFT codes allows us to process payments and provide seamless billing services for using any of our products or services;
- 3.3.3** To manage communication with you and respond to any of your queries or concerns. By processing interactions such as phone calls, emails, and biometric data, we can respond promptly to inquiries and improve customer experience. Recording conversations also helps with quality assurance and resolving disputes.
- 3.3.4** To ensure a safe and secure environment for all visitors, employees, and stakeholders;
- 3.3.5** Carrying out credit checks and credit scoring;
- 3.3.6** Keeping you informed generally about our services;
- 3.3.7** to comply with any legal, governmental or regulatory requirements;

3.3.8 Preventing and detecting fraud or other crimes and for debt recovery;

3.3.9 For research, statistical, survey and other scientific or business purposes including commercialization.

3.3.10 Where you attend an event sponsored by Kenya Power, photos or videos of the event will be taken. These images or videos may be used to share news about the event in press releases, printed publicly, and/or published on our website and social media channels.

3.3.11 Where you have applied for employment at Kenya Power, we perform applicant screening and background checks.

3.3.12 Where you are a Kenya Power employee (including contractors), we create an employment record of you on our system to facilitate continuous monitoring during your employment with us.

3.3.13 Where you are a Kenya Power director or shareholder, we create a record of you as a director/shareholder in our system.

3.3.14 Where you are a supplier to Kenya Power, we process your personal information for due diligence, risk assessment, administrative and payment purposes.

3.3.15 Provide aggregated data (which do not contain any information which may identify you as an individual) to third parties for research and scientific purpose;

3.4 Categories of Data

Categories of Personal Data as defined in the Data Protection Act, 2019 of Kenya may be processed for various reasons.

3.5 Lawful Basis for processing your information

We will process your personal information based on any of the lawful basis provided for under the Data Protection Act as outlined below:

3.5.1 The performance of a contract to which you are a party;

3.5.2 For compliance with any legal obligation in which Kenya Power is under an obligation to comply;

3.5.3 For the performance of a task carried out in the public interest or in the exercise of official authority vested in Kenya Power;

3.5.4 Kenya Power's legitimate business interests;

3.5.5 Consent you provide;

3.5.6 To protect your vital interests or vital interests of any natural person.

3.6 Retention of data

We will retain your personal data only as long as necessary to fulfil the purposes for which it was collected, including any legal, regulatory, tax, or reporting requirements. If there is a complaint or potential litigation, we may retain your data for a longer period.

To determine how long to keep your data, we consider factors such as its nature, sensitivity, potential risks, and whether we can achieve the same purposes through other means. We also take into account our internal policies and applicable legal requirements on retention of data.

Anonymized data, which can no longer be linked to you, may be kept indefinitely.





4.0 Disclosure of Information

4.1 Any request for disclosure of your personal data information shall be in accordance with applicable legal and regulatory requirements. Kenya Power shall assess and review each request for personal data and may decline to disclose or share such information to the requesting party.

4.2 We may disclose your information to:

4.2.1 Law-enforcement agencies, regulatory authorities, courts or other statutory authorities in response to a demand issued with the appropriate lawful mandate and where the form and scope of the demand is compliant with the law

4.2.2 our associates, service providers, software developers or agents who are involved in delivering Kenya Power products and services you may require;

4.2.3 Fraud prevention and Anti money laundering agencies;

4.2.4 publicly available and/or restricted government databases to verify your identity information in order to comply with regulatory requirements;

4.2.5 Survey agencies that conduct surveys on behalf of Kenya Power;

4.2.6 Any other person that we deem legitimately necessary to share the data with.

4.3 We shall not release any information to any individual or entity that is acting beyond its legal mandate.

4.4 We will get your express consent before we share your personal data with any third party for direct marketing purposes.



5.0 Access to and Updating your Information

To update your information, visit any Kenya Power office near you to change how we get in touch with you and your account details whenever you like. You can also write to dpo@kplc.co.ke for updating of your information.

6.0 Safeguarding and Protection of Information

Kenya Power has put in place technical and operational measures to ensure integrity and confidentiality through among others: access control, physical and environmental security and monitoring and compliance.

7.0 International Data Transfers

From time to time we may need to transfer your personal information outside the Republic of Kenya.

Where we send your information outside Kenya, we will make sure that your information is properly protected in accordance with the applicable Data Protection Laws.

8.0 Your Rights

Subject to legal and contractual exceptions, you have rights under data protection laws in relation to your personal data. These are listed below: -

- 8.1** Right to be informed of the use to which your personal data is to be put;
- 8.2** Right to access your personal data in custody of Kenya Power;
- 8.3** Right to object to the processing of all or part of your personal data;
- 8.4** Right to correction of false or misleading data; and
- 8.5** Right to deletion of false or misleading data about them.
- 8.6** Right to request transfer of your personal data in [an electronic format].

If you wish to exercise any of the rights set out above, please contact us on **dpo@kplc.co.ke**.

We try to respond to all legitimate requests within reasonable time. Occasionally it could take us longer if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

9.0 How to Contact Us

If you have any questions or concerns regarding how your personal data is processed, you can email us on **dpo@kplc.co.ke**.

As a Data Controller below are the contact details of our Data Protection Officer:

Data Protection Officer
dpo@kplc.co.ke
The Kenya Power & Lighting Company PLC
Stima Plaza
Kolobot Road,
P.O Box 30099- 00100, Nairobi
www.kplc.co.ke





10.0 Right to Lodge Complaint

You have the right to lodge a complaint with the Office of the Data Protection Commissioner, the relevant supervisory authority that is tasked with personal data protection within the Republic of Kenya.

11.0 Non-Compliance with this Statement

Kenya Power shall have the right to terminate any agreement for failure to comply with the provisions of this Privacy statement and reject any application for information contrary to this statement.

12.0 Amendments to this Statement

Kenya Power reserves the right to amend or modify this statement at any time. If Kenya Power amends this statement, You can access the most current version of the privacy statement on our website. Any amendment or modification to this statement will take effect from the date of notification on the Kenya Power website.



Data Sharing Guidelines



Data Sharing Guidelines

1.0 Introduction

These Data Sharing Guidelines (“Guidelines”) are pursuant to and in compliance with Section 55 of the Data Protection Act, 2019. They outline the principles for sharing data within and outside of Kenya Power. The aim is to ensure that data is shared in a secure and compliant manner, in line with data protection laws, thereby protecting privacy of individuals and integrity of the data.

Sharing of personal data raises a number of concerns, including privacy, security, and confidentiality of such data as it may lead to unauthorized access, use or disclosure, contravening provisions of the Data Protection Act, 2019.

Recognizing the risks associated with unauthorized access and disclosure of personal data, it is imperative to establish clear guidelines on sharing personal data within the Company and with external or third parties.

2.0 Scope

The guidelines apply to all employees, contractors, and third-parties who handle/process data on behalf of Kenya Power. They apply to all types of personal data, sensitive personal data, and any other proprietary or confidential information.

3.0 Basis for Sharing Personal Data

The following principles and basis shall govern the sharing of personal data within and by the Company:

3.1 Consent: Data subjects shall give explicit permission/consent for their personal data to be shared. The consent must be informed, specific, and freely given. Consent can be withdrawn at any time.

3.2 Contractual Necessity: Personal data may be shared when it is necessary for the performance of a contract with the individual, or to take steps prior to entering into a contract. For example, sharing data to fulfil a service that the person has signed up for e.g customers, new employees, suppliers, contractors and other service providers.

3.3 Legal Obligation: personal data can be shared when it is necessary to comply with legal obligations, such as fulfilling regulatory requirements, responding to law enforcement requests, or complying with a court order.

3.4 Vital Interests: Personal data can be shared when it is necessary to protect someone's life or physical well-being, or for other vital interests, such as in emergency situations.

3.5 Legitimate Interests: personal data can be shared if there is a legitimate interest, provided that interest is not overridden by the individual's rights and freedoms. This might include cases such as fraud prevention.





3.6 Performance of a task carried out in the public interest or in exercise of official Authority vested in Data Controller: Personal data may be shared if it is necessary for carrying out a task that is in the public interest or in the exercise of official authority. This can include sharing data for public health reasons, law enforcement, or other governmental functions.

4.0 Types of Data

The following types of data are subject to these guidelines:

4.1 Personal Data: Any information relating to an identified or identifiable individual (e.g., names, contact details, and identification numbers).

4.2 Sensitive Personal Data: Data that is particularly private and requires enhanced protection (e.g., health data, financial information, racial or ethnic data).

4.3 Confidential Business Data: Proprietary or business-sensitive information that could harm the Company if disclosed (e.g., trade secrets, business plans, etc.).

4.4 Public Data: Data that is intended for public consumption and can be freely shared without restrictions.

5.0 Guidelines for Internal Data Sharing

5.1 Access Control: Data should only be accessed or shared with employees or departments who need it to perform their job duties. The Company shall implement role-based access controls to ensure that only authorized individuals have access.

5.2 Data Encryption: Internal data sharing must be done using secure channels (e.g., encrypted emails, secure file transfer protocols, internal databases with access controls).

5.3 Audit Trails: the Company shall keep system logs of who accessed or modified data to ensure accountability and traceability. Regular audits shall also be conducted to ensure compliance.

5.4 Data Integrity: the Company shall ensure that the data shared internally is accurate and up to date. Any discrepancies or data errors shall be addressed promptly.

6.0 Guidelines for External Data Sharing

When sharing data with external parties (Law-enforcement agencies, regulatory authorities, service providers, contractors, agents etc.), the following guidelines shall be adhered to:

6.1 Format of requests: all requests for sharing personal data with external or third parties shall be in writing and shall specify:

- The purpose for which the personal data is required
- The duration for which the personal data shall be retained
- Proof of safeguards put in place to secure personal data from unlawful disclosure.

6.2 Basis for sharing personal data: requests for personal data by external or third parties may be processed under certain circumstances such as where there is consent of the data subject or production of valid court orders. Other basis for sharing such personal data is outlined under Clause 3 above. If uncertain whether or not to share personal data, please contact the Data Protection Officer at dpo@kplc.co.ke.

6.3 Data Sharing Agreements: A formal Data Sharing Agreement shall be signed before sharing personal data with external or third parties. The Data Sharing Agreement will clearly outline the purpose of the data sharing, the responsibilities of each party, and compliance with relevant laws and regulations.

6.4 Data Anonymization/De-identification: If possible, the Company shall share anonymized or de-identified data to reduce privacy risks. This is in cases such as where aggregated data is required or data is required for historical, journalistic or research purposes. If data needs to be shared in identifiable form, the Company shall ensure that the external or third party has adequate technical and organizational measures in place to secure personal data from unlawful disclosure.

6.5 Secure Data Transfer: the Company shall use secure methods to share data with external or third parties, such as encrypted emails, password - protected files, coded data, secure file sharing platforms, or virtual private networks (VPNs).

6.6 Third-Party Compliance: the Company shall ensure that external or third-party recipients of the data comply with security and data privacy requirements outlined under the Data Protection Act, 2019 and the regulations. This may involve periodic audits or assessments of the third party's practices.



7.0 Data Protection and Security

7.1 Data Encryption: All sensitive and personal data shall be encrypted or coded once processed into Kenya Power systems and while being shared to prevent unauthorized access.

7.2 Authentication: The Company shall implement strong authentication protocols (e.g., multi-factor authentication) for systems that handle or share personal data.

7.3 Access Control: the Company shall ensure that access to data is restricted based on the principle of least privilege (i.e., only those who need access to data to perform their job functions should have it).

7.4 Monitoring and Auditing: the Company shall continuously monitor systems and activities related to data sharing. The Company shall also implement audit logs to track data access, modifications, and sharing of data.

7.5 Data Breach Protocols: In the event of a data breach, the Data Protection Officer should be notified immediately at dpo@kplc.co.ke. The incident response plan shall be followed, which includes notifying affected parties and the Office of the Data Protection as required.

8.0 Training and Awareness

8.1 Employee Training: All employees shall undergo training on Data Privacy and Data Sharing Guidelines. Regular refresher courses shall also be undertaken to keep employees updated on emerging requirements and best practices.

8.2 Awareness Campaigns: the Company shall raise awareness on the importance of data protection and the Company's data sharing policies through internal communications and workshops.

9.0 Enforcement and Consequences

9.1 Violations: Violations of these guidelines may result in disciplinary action, including termination of employment, legal enforcement actions (civil or criminal proceedings), or termination of contracts with third-parties.

9.2 Reporting Violations: Employees or contractors who observe a breach of these guidelines should report it immediately to the Data Protection Officer at dpo@kplc.co.ke.



Access Control Guidelines



Access Control Guidelines

1.0 Introduction

These guidelines define the access control framework for the Company, ensuring that access to information systems and data is granted based on principles of least privilege, need-to-know, and role-based access. The guidelines aim to protect the confidentiality, integrity and security of the information/data held by the Company.

2.0 Scope

These guidelines apply to all employees, contractors, and third-party users who need or have access to Kenya Power's data contained in the systems. They govern the process of access to classified personal data.

3.0 Definitions

3.1 Access Control: The process of granting or restricting access to data within the Company.

3.2 Authentication: The process of verifying a user's identity through credentials such as passwords, biometrics, or tokens.

3.3 Authorization: The process of determining the user's access level or permissions after authentication.

3.4 Data Classification: is the process of assigning labels to data based on its sensitivity, risk or confidentiality.

3.5 Data Labelling: is the process of adding metadata or tags to data to describe its attributes. The Company shall classify data as public, internal, confidential, top-secret/highly confidential.

3.6 Least Privilege: A security principle that restricts or limits access of data to the minimum level only necessary to perform their job.

3.7 Role-Based Access Control: A method for managing access based on user roles within the Company.

4.0 Access Control Principles

4.1 Least Privilege: Users will be granted the minimum level of access required to perform their job responsibilities.

4.2 Multi-Factor Authentication: a security method that requires users to provide more than one form of identification such as a password and a temporary passcode to access a system.

4.3 Need-to-Know: Access to sensitive personal data and systems will be granted only to individuals who need it to perform their official tasks.

4.4 Role-Based Access Control: Access to information and data will be granted based on the roles assigned to users.

4.5 Segregation of Duties: Critical tasks shall be divided among multiple users to reduce the risk of fraud or errors.

5.0 Data Classification

5.1 The elements of Data Classification shall be as follows:

5.1.1 Content-based: Labels are applied based on the contents of the data.

5.1.2 Context-based: Labels are applied based on metadata, such as the creator of the data or the program used to create it.

5.2 Classification will be outlined in KPLC's Data Classification Manual

5.3 Upon Data Classification, security measures shall be tailored and applied based on each data category's need.





6.0 User Account Management

6.1 Account Creation: All user accounts shall be requested and approved by the relevant departmental managers. The user's role and responsibilities will determine the level of data access.

6.2 Account Modification: Any modification to user access rights must be approved by departmental managers and documented. This includes changes in roles, access levels, and privileges.

6.3 Account Termination: User accounts must be deactivated or removed immediately upon termination of employment, contract expiration, or when access is no longer needed.

6.4 Account Review: Regular reviews of user accounts and data access levels will be conducted every three months to ensure appropriate data access is maintained.




7.0 Authentication and Authorization

7.1 Strong Authentication: System users holding sensitive personal data shall authenticate using strong methods such as multi-factor authentication where feasible.

7.2 Password Policy: Passwords shall be complex, with a minimum length of 8 characters and shall include a combination of uppercase letters, lowercase letters, numbers, and special characters. Passwords must be changed every 30 days.

7.3 Role and Permission Review: User roles and permissions will be reviewed regularly to ensure they remain aligned with their job descriptions.



8.0 Data Leakage Prevention (DLP):

The Company shall implement robust DLP initiatives/solutions across systems like INCMS, FDB, IPMP, and DCS.

9.0 Masking/Coding of Personal Data


9.1 Data Masking: Upon submission or collection of personal data into the system, the data shall be immediately masked or anonymized where necessary to minimize the risk of unauthorized access or exposure.

9.2 Data Decoding: Personal data shall only be decoded or rendered readable by authorized personnel or systems in cases where it is necessary for the performance of specific tasks.

9.3 Access Controls: Only individuals with the necessary authorization shall have access to the unmasked or decoded personal data.

9.4 Access logs: All such accesses shall be logged and monitored to ensure authorized access and compliance with data protection requirements.

9.5 Encryption: Where applicable, personal data will be encrypted at rest and in transit to provide an additional layer of security against unauthorized access during storage or transmission.





10.0 Access Levels and Permissions

10.1 Administrative Access: Only authorized personnel (system administrators) shall be permitted to access and modify system configurations, perform maintenance, and manage security settings.

10.2 Standard User Access: Standard users will have access to only that data required to perform their duties, with access logs generated to ensure access to personal data is on a need-to-know basis.

10.3 Restricted Access: Access to sensitive personal data (top-secret/highly confidential) will be restricted to individuals with a valid need to know, based on their role and authorization.

11.0 Monitoring and Auditing

11.1 Access Logging: There shall be access logs to all critical systems and information with personal data for audit purposes. Access logs shall include user IDs, timestamp of access, actions performed e.g modification of data, and the system or data accessed.

11.2 Regular Audits: Regular audits of access logs will be conducted on a monthly basis to identify any unauthorized access or violation of these guidelines.

11.3 Incident Reporting: Any unauthorized access or breach incidents shall be reported to the Security Department immediately for investigation.

12.0 Enforcement and Compliance

12.1 Violations: Violations of these guidelines may result in disciplinary action, including termination of employment, legal enforcement actions (civil/criminal proceedings), or termination of contracts with third-parties.

12.2 Compliance: The Company will comply with legal and regulatory requirements and industry standards concerning access controls.

12.3 Reporting Violations: Employees or contractors who observe a breach of these guidelines should report immediately to the Data Protection Officer at dpo@kplc.co.ke.



Data Breach Handling Guidelines



Data Breach Handling Guidelines

1.0 Introduction

The purpose of these guidelines is to define the Company's approach to identifying, responding to, and managing Data Breaches. The objective is to ensure timely and effective action is taken to mitigate the impacts of a Data Breach, protect individuals' privacy, comply with legal and regulatory requirements, and prevent future occurrences.

2.0 Scope

These guidelines apply to all employees, contractors, third-parties with access to the Company's data and systems. They cover all forms of Data Breaches involving sensitive or personal data, whether the breach is accidental or intentional.

3.0 Definitions

3.1 Personal Data: Any information that can identify a living individual (e.g., name, address, identification number, email).

3.2 Personal Data Breach: A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

3.3 Sensitive Personal Data: Data that requires special protection, such as financial data, health records, 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 sexual orientation of a data subject.

3.4 Incident Response Team (IRT): A team of designated personnel responsible for managing and responding to incidents and Data Breaches.

4.0 Responsibilities

4.1 Data Protection Officer (DPO): The DPO is responsible for overseeing the implementation of these guidelines, managing Data Breach incidents, and ensuring compliance with relevant laws with regard to regulatory reporting of breaches.

4.2 Incident Response Team: Comprised of the DPO, ICT, Security and any other relevant stakeholders shall be responsible for investigating the breach, containing the incident, and implementing technical controls to prevent further exposure.

4.3 Employees: All employees shall immediately report any suspected Data Breach to the DPO at dpo@kplc.co.ke



5.0 Identifying and Reporting Data Breaches

5.1 Detection: Any suspected or confirmed Data Breach shall be reported to the DPO immediately. Employees shall be trained to recognize indicators of Data Breaches. A Data Breach is identified when there is an unauthorized access to, disclosure, alteration, or destruction of personal or sensitive data. It may be identified by:

5.1.1 A report from a third-party or customer about potential data loss or exposure.

5.1.2 Alerts generated by Data Leakage Prevention solutions and similar technologies.

5.1.3 Employees, contractors, or other stakeholders noticing or suspecting unauthorized access to data.

5.2 Do Not Alter Evidence: if a potential or confirmed Data Breach occurs, preserve all relevant evidence, including access logs, screenshots, and any other materials, in their original form for further investigation

5.3 Reporting: In the event of a Data Breach within the Company, it will immediately be reported to the DPO.

6.0 Key Information to Include when Reporting a Data Breach

When reporting a Data Breach, the following critical details shall be included to ensure swift identification and response:

6.1 Date and Time: When the breach was first identified or suspected.

6.2 Description of the Incident: A detailed description of the breach, including what happened, how the data was accessed or exposed, and the data involved (e.g., personal data, financial data, sensitive personal data).

6.3 Affected Systems or Data: Identify which systems, applications, or types of data are impacted (e.g., employee records, customer information).

6.4 Potential Impact: Indicate the potential impact of the Data Breach on the Company and affected individuals (e.g., severity, number of people affected, defrauding of a customer).

6.5 Immediate Actions Taken: Indicate immediate actions taken (if any) to contain the breach

6.6 Suspected Cause: If known, indicate any potential causes of the Data Breach (e.g., cyber-attack, human error, physical theft etc).



7.0 Data Breach Response Procedure

7.1 Acknowledge the Report: The DPO will confirm receipt of the breach report to the individual (s) who reported it.

7.2 Initial Assessment: The Incident Response Team will conduct an initial evaluation to determine if the event qualifies as a Data Breach and assess the severity.

7.3 Containment: if it is determined that the event qualifies as a Data Breach, the Incident Response Team shall contain the Data Breach.

7.4 Assessment: The Incident Response Team shall evaluate the scope and extent of the breach, the person(s) responsible for the breach, the type of data affected, how it was accessed, and the potential impact on data subjects and the Company.

7.5 Communication: The Incident Response Team shall notify key stakeholders (e.g., executive management, affected departments).

7.6 Investigation: A detailed investigation shall be conducted to determine the root cause of the Data Breach and identify any vulnerabilities that might have been exploited. All actions taken during the investigation shall be documented, including findings, timelines, and recommendations made.

7.7 Mitigation: Measures to prevent the breach from escalating or recurring shall be implemented. This includes reinforcing vulnerabilities, enhancing access controls, or blocking unauthorized access points.

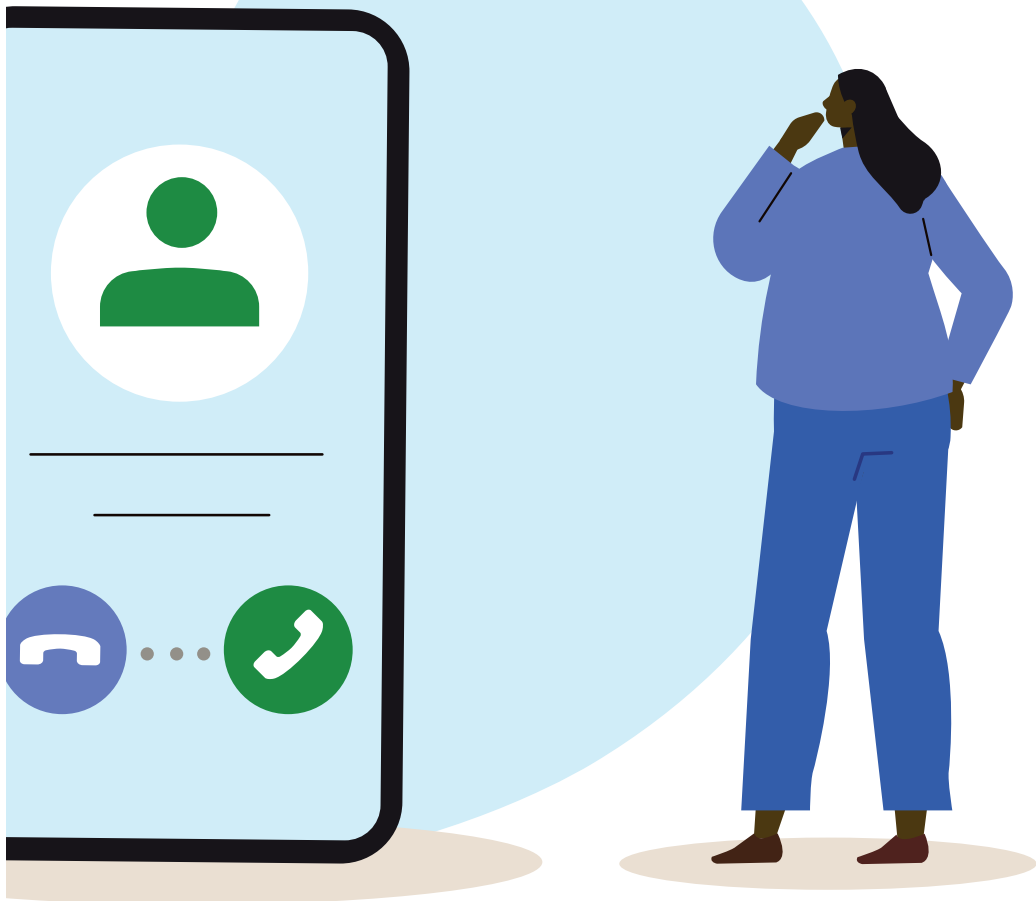
8.0 Notification Requirements

8.1 Office of the Data Protection Commissioner. The Company shall notify the Data Commissioner within seventy-two (72) hours of becoming aware of a breach. In notifying the Data Commissioner, the Company will provide details of the breach, actions taken, and any steps taken to prevent future incidents.

8.2 Data Subject (Affected Individuals): The Company shall communicate to the data subject in writing as soon as possible of the Data Breach, unless the identity of the data subject cannot be established. Notifications to data subjects on Data Breaches will include:

- 8.2.1** The nature of the breach
- 8.2.2** The categories of affected data
- 8.2.3** The likely consequences of the breach to the data subject
- 8.2.4** Actions the individual (s) should take to protect themselves
- 8.2.5** Measures taken by the Company to address the breach

8.3 Third Parties: If third-party vendors, contractors, or business partners are impacted, they will be informed promptly.



9.0 Documentation of Incidents:

The Company will maintain a detailed record of each Data Breach, including all steps taken during the breach response such as the timeline of events, individuals notified, corrective actions taken, and lessons learned for legal and compliance purposes.

10.0 Post-Incident Review

10.1 Root Cause Analysis: After containment of the breach, a comprehensive review will be conducted by the Incident Response Team to understand the root cause of the breach and identify any gaps in the Company's data controls.

10.2 Preventive Measures: The Company will implement corrective measures to prevent similar incidents, including review of Data Protection Policies and Procedures, enhancing employee awareness, improving security protocols, reinforcing vulnerabilities, or enhancing monitoring systems.

10.3 Reporting to Executive Management Committee: A final report will be submitted to the Executive Management Committee, detailing the breach, its impact, and corrective actions.

10.4 Training and Awareness: Based on the Data Breach and its causes, additional training will be provided to relevant employees and stakeholders to raise awareness on how to mitigate risks in the future.

11.0 Training and Awareness

11.1 Employee Training: Employees will undergo regular training on data security and how to recognize and report confirmed or potential Data Breaches.

11.2 Awareness Campaigns: Periodic campaigns will be conducted to raise awareness within the Company and its customers about data security and the procedures for handling Data Breaches.

12.0 Enforcement and Compliance

12.1 Violations: Violations of these guidelines may result in disciplinary action, including termination of employment, legal enforcement actions (civil or criminal proceedings), or termination of contracts with third-parties.

12.2 Reporting Violations: Data Subjects, employees and contractors who observe a breach of these guidelines should report it immediately to the Data Protection Officer at dpo@kplc.co.ke



Frequently Asked Questions



Frequently Asked Questions

1. What is data protection?

Data protection is about keeping personal information that can identify an individual safe and secure from being accessed or used by unauthorized people.

2. Why is data protection important?

Data protection is crucial for building trust, preventing financial fraud and other forms of misuse, and ensures compliance with data protection laws, thereby preventing data breaches and associated penalties.

3. What is a data breach?

It is the unlawful or unauthorized access or disclosure of personal data.



4. What is the effect of data breaches to the Company?

Data breaches can result in reputational damage to Kenya Power, litigation cases, and financial penalties of up to 5 million Kenya Shillings for each data breach.

Disciplinary action will be taken against employees involved in data breaches as per the Company's HR Policies.

5. Who is responsible for data protection?

Data protection is every employee's responsibility. From employees handling customer and employee information to IT teams securing systems, we all play a role in safeguarding personal data.

6. What are some examples of personal data?

Examples of personal data include names, addresses, phone numbers, images, health status, biometric data, property/salary details, marital status, and family details, including names of the person's children, parents, spouse or spouses, etc.

7. Where Does Data Protection Apply?

Data protection applies everywhere personal data is handled—whether in the office, on email, in printed documents, on company systems, mobile devices, or even in conversations. It includes both physical and digital environments, at work and in the field.

8. How do employees ensure data protection?

- Ensure you do not share your colleague's, customer's or any other individual's personal data without their explicit consent.
- If you suspect or identify any data breach, report it immediately to the Data Protection Officer (DPO) at dpo@kplc.co.ke. Prompt reporting is crucial in preventing further exposure and mitigating risks.
- Use strong unique passwords and avoid sharing passwords with anyone.
- Ensure secure storage of devices and documents containing personal data and never leave such documents unattended or on your desk.
- Only access or share personal data when it is necessary for the performance of your duties.
- In the event of loss of your laptop or any device containing personal data, immediately notify ICT and the DPO to ensure the information in the device is erased and not accessed by unauthorised third parties.
- Complete mandatory data protection training and assessments.
- Familiarise yourself and ensure adherence to the Company's Data Protection Policy and procedures.

Direct all request for personal data from third parties to the Data Protection Officer (DPO) at dpo@kplc.co.ke



Kenya Power

The Kenya Power and Lighting Company Plc


www.kplc.co.ke


USSD *977#


97771


Kenya Power Care


Kenya Power


kenyapower


@kenyapower



***Safeguarding Data,
Upholding Trust***

