	ABUJA ELECTRICITY DISTRIBUTION PLC **DATA PROTECTION POLICY**			
Title:	**DATA PROTECTION POLICY**			
Policy No.:	**AEDC/ICT.5/068/2019**	**Issue No. 1.0**	**Date: 25th July 2019**	**Status: Approved**

	DESIGNATION	**NAME**	**SIGNATURE**	**DATE**
Document Owner(s):	**Data Protection Officer**	**Michael Olugbemi**		
Final review by:	**Chief Information Officer (CIO)**	**Samuel Kyakilika**		
Final review by:	**Chief Risk Officer (CRO)**	**Collins Mulenga Chabuka**		
Final review by:	**Chief Internal Auditor (CIA)**	**Ahmed Rufai Salau**		
Final review by:	**Director, Legal Services & Company Secretary**	**Olajumoke Delano**		

Approved by: _____ MD/CEO	Date: _____

Contents

1.0 Our Commitment

Abuja Electricity Distribution PLC (AEDC) understands that the personal data used for business activities should be secured and it is our responsibility to keep it confidential for the company to be trusted.

In the course of carrying out our business activities, we obtain, use and protect certain data about individuals (data subjects) for operational and business reasons. Employees/third parties may have access, handle or process personal data concerning colleagues, customers, vendors and board members. It is essential that AEDC protects personal data and ensure that the requirements stipulated by the Nigeria Data Protection Regulation 2019 (NDPR) are complied with.

Personal data which we/others access, hold, collect and process on behalf of AEDC shall only be used for legitimate AEDC business purposes. Sensitive personal data shall be handled with care and in a confidential manner. This is data relating to an individual's medical records, gender, ethnicity, state of origin, political/religious beliefs, home address, details of relatives/dependents and any biometric data(e.g. bank account details, BVN, Phone number) processed to uniquely identify a person.

2.0 Context

Data Protection Regulation/Laws now exist in various countries around the world. Penalties for breach of such laws and regulations can be severe and may result in significant fines and/or criminal charges for AEDC (based NDPR 2019). The Nigeria Data Protection Regulation (NDPR) 2019 describes how organizations within Nigeria - including AEDC, shall collect, handle and store personal data

As an employer, we process personal data about our employees and their family members for employment administration purposes, for recruitment and background checks, performance management, payroll, pension administration and other uses. We also handle the personal data of our customers, vendors, contractors and business partners for business purposes; including customer and vendor administration, credit checks.

This data may be kept in paper format or electronically.

We understand that in the areas where we handle and process personal data of employees, customers, contractors, vendors and third parties, it is our responsibility to follow the Data Protection Principles as guided by the NDPR.

This Data Protection Policy framework ensures:

- AEDC complies with Data Protection Regulation (NDPR) and follows good practice standards
- AEDC protects the rights of staff, customers, vendors, third parties and other stakeholders with regards to their personal data
- AEDC is transparent about how it accesses, collects and process personal data
- AEDC protects itself as an organization from the risks of personal data breach

3.0 Definitions

The Company	Abuja Electricity Distribution Company (AEDC)
NDPR	Nigeria Data Protection Regulation 2019
Personal Data	According to 'NDPR' means any data relating to an identified or identifiable natural person (data subject); It can be anything from a name, address, a photo, an email address, bank details, posts on social networking websites, medical data, and other unique identifier such as but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.
Data Subject Access Request	Means the process for an individual to request a copy of their data under a formal process and payment of a fee
Data Subjects	Under this Data Protection Policy is any person, who can be identified, directly or indirectly, by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"

DPO	Data Protection Officer
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction
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
Responsible Person	The person responsible for handling data within the department or company.

4.0 General Provisions of the Policy

a. This policy applies to all personal data collected, stored, transmitted and processed by AEDC.

b. All Directors are responsible for ensuring that staff within their area of responsibility comply with this policy via proper implementation of appropriate processes, controls, training and compliance.

c. Our Business partners who process personal data on our behalf are mandated to observe the principles in this policy

d. The company shall register (where required) with relevant regulatory authorities as an organisation that processes personal data.

e. AEDC Employees, Customers, Vendors, Contrators and other relevant stakeholders shall comply with the company's data protection measures:

- When working with personal data and other sensitive data, employees should ensure the screens of their computers are locked when left unattended;

- Personal data shall not be shared without proper authorization.
- Personal data shall always be captured with consent from the data subject
- Data shall be encrypted when stored or transmitted electronically.
- Personal data captured shall be processed in a secured environment and by authorized persons.

5.0 Data Protection Principles

AEDC data protection principles are as follows:

a. Data collection and processing: AEDC shall obtain and process personal data lawfully, fairly and in a transparent manner. This means AEDC shall ensure a legal basis for obtaining and processing personal data and inform individuals what categories of personal data have been collected, or will collect, and explain the purpose(s) for which their personal data will be used.

b. Purpose Limitation: AEDC shall collect personal data for specified, explicit and legitimate purposes only or uses as permitted by law after seeking data subject's consent and ensure it is not further processed in a manner that is incompatible with those purposes

c. Minimisation: The personal data handled by AEDC shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are collected. AEDC shall securely destroy or delete redundant or excessive data in line with applicable data retention policy.

d. Accuracy: Personal data should be accurate and, where necessary, updated.

e. Storage Limitation: Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods so far it will be processed solely for archiving purposes (i.e. public interest, scientific or historical research or statistical purposes) subject to implementation of the appropriate organisational measures required by the NDPR in order to safeguard the rights and freedoms of individuals

f. Confidentiality and Integrity: Personal data collected by AEDC shall be processed in a manner that ensures confidentiality , integrity and appropriate security of

the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate organisational measures.

g. Accountability: AEDC shall be able to demonstrate its compliance to the NDPR 2019.

5.1 Offline data storage

a. When data is stored on paper, it shall be kept in a secured storage where it cannot be illegally accessed.
b. This Policy also applies to data that has been archived electronically.
c. Employees/Vendors/and Contractors will make sure paper and printouts are not exposed.
d. Discarded printouts shall be shredded and disposed-off securely.

5.2 Online data storage

When data is stored electronically, it shall be protected from unauthorized access, accidental deletion and malicious hacking attempts.

AEDC Employees, Vendors, and Contractors shall comply with requirements as stipulated in AEDC's Information Security Policy.

5.3 Confidentiality, Integrity and Accountability

a. Personal data of individuals shall be handled and processed with appropriate confidentiality and ensure data integrity.
b. Accountability of handling and processing personal data necessitates the following;
    - The appointment of a Data Protection Officer (s)
    - Develop Privacy Impact Assessment (PIA). The PIA should be done initially to ensure any new processing activity involved in the handling of personal data is designed to comply with the Data Protection Principles
    - Third Party Data Handling. The disclosure and/or transfer of personal data to third parties should not occur unless an agreement/contract exists

confirming that AEDC shall keep data confidential and ensure that appropriate security measures are in place

- International Data Transfer reports: AEDC shall ensure security in transferring personal data from one country to another.

5.4 Individual rights

a. Data subjects also have the right to object to the use of their personal data for non-essential purposes. Any such requests should be made via email to data.protection@abujaelectricity.com

b. Data subject(s) may ask AEDC to access, amend, obtain a copy or delete personal data (subject to terms and condition) that are handled and processed on their behalf. Any such requests shall be made via email to data.protection@abujaelectricity.com and shall be dealt with in 30 calendar days.

5.5 Data Security

a. All systems that hold personal data should have well-managed and documented organisational access controls and protocols and ensure any bulk personal data removed from the system is appropriately secure (encrypted).

b. When personal data is deleted, it shall be done safely such that the data is irrecoverable.

c. Appropriate back-up and disaster recovery solutions shall be in place.

d. AEDC shall provide employees with online privacy and data security training.

e. AEDC shall Establish clear procedures for reporting data/privacy breaches or data misuse

f. Data protection audits/assessments shall be conducted at least twice every year.

6.0 Policy Governance

- This policy shall be reviewed at least once annually
- The Responsible Person (Data Protection Officer) shall take responsibility for the company's ongoing compliance with this policy
- The Data Protection Officer's duties shall include the following:
  - Ensure that the organization adheres to the NITDA Guidelines.
  - Ensure continued adherence to data protection and privacy policies and procedures.
  - Ensure that personal data is protected and providing for effective oversight of the collection and use of personal data.
  - Ensure effective data protection and data management within the organization and ensure compliance with the privacy and data security policies.
  - Create awareness, recommended practices and provide training for employees/contractors/third party to promote compliance with the privacy and data security policies.

7.0 Monitoring

AEDC shall monitor how personal data is collected, stored, processed and transmitted and should be done in compliance with applicable regulations.

Any breach of this Policy shall be considered to be a breach of the AEDC Code of Business Conduct and shall be reported immediately.

- Employees shall report non-compliance concerns or any breach to their Line Manager/Supervisor, Data Protection Officer, HR, Legal Service or the Risk and Compliance Department
- Data incidents (e.g. unauthorized access to, disclosure of, loss or theft of personal data), including those relating to any third party or business partner, shall be reported to Data Protection Officer and AEDC Legal Service Department immediately
- As required by the NDPR, In the event of a breach of security leading to the accidental or unlawful alteration or unauthorized disclosure of, or access to, personal data, the company shall promptly contact the relevant supervisory

authority (NITDA) within 72 hours of becoming aware of the breach, where feasible

- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, AEDC shall inform those individuals without undue delay
- The company shall also keep a record of any personal data breaches
- All staff, and others processing personal data on the company's behalf shall read this policy. A failure to comply with this policy will result in disciplinary action.
- Any deliberate, willful or negligent breaches of this policy by an employee or contractor or third party shall be dealt with in accordance with the NDPR, AEDC Investigations and Disciplinary Guidelines, as permitted by law.