BEDC Electricity PLC
5, Akpakpava Street, Benin City, Edo State, Nigeria

Policy Area	Information		
Title of Policy	**DATA PROTECTION POLICY**		
Reference No.			
Version	1.0		
Policy Owners	All Staff of BEDC		
No. of Revision	0		
Date of Draft	29th September 2022		
Effective Date			
Approve By	*Role*	*Name*	*Signature/Date*
	MD/CEO	**Dr. Henry Ajagbawa**	
	Board of Directors		

1.0 INTRODUCTION

BEDC as a utility company needs to collect and process personal data about people with whom it deals to carry out its business and provide its services. Such people include but are not limited to employees (past, present, and prospective), customers, suppliers/contractors, and other business contacts. The data may include identifiers such as name, address, email address, date of birth, phone number, national identity number etc. It may also include private and confidential information, and special categories of personal data such as race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health data, gender history, and criminal data.

2.0 PURPOSE

BEDC Data Protection Policy refers to our commitment to treat information no matter how it is collected, recorded, and used (e.g., on a computer or other digital media, on hardcopy, paper, or images, including CCTV) of employees, customers, stakeholders and other interested parties with the utmost care and confidentiality in line with the Nigeria Data Protection Regulation (NDPR).

With this policy, BEDC will ensure that it gathers, stores and handles data fairly, transparently, with respect towards individual rights and to protect itself from the risks of data breach to maintain the confidence of our service users and employees.

3.0 SCOPE

This policy refers to all employees, customers, suppliers/contractors, applicants etc. who provide any amount of information to BEDC.

BEDC employees must adhere strictly to this policy. Contractors, consultants, partners, and other external entities are also covered. Generally, this policy applies to anyone BEDC collaborates with, or who acts on our behalf and may need occasional access to data.

4.0 POLICY

BEDC fully supports and must be able to demonstrate compliance with the Nigeria Data Protection Regulation which are summarized as follows:

4.1 Fairness and Lawfulness

- When processing personal data, the individual rights of the data subjects must be protected. Personal data must be collected and processed in a legal and fair manner.

- Collected data shall be adequate, relevant, and not excessive in relation to the purposes for which they are obtained and their further processing.

- Individual data can be processed on voluntary consent of the person concerned.

4.2 Restriction to a specific purpose

- Personal data can be processed only for the purpose it was defined before the data was collected. Personal data shall be obtained for specified, explicit and legitimate purposes, and shall not subsequently be processed in a manner that is incompatible with those purposes. Subsequent changes to the purpose are only possible to a limited extent and require justification.

- However, further data processing for statistical, scientific, and historical purposes shall be considered compatible with the initial purposes of the data collection, if it is not used to take decisions with respect to the data subjects.

4.3 Transparency

- The data subject must be informed of how his/her data is being handled. In general, personal data must be collected directly from the individual concerned. When the data is collected, the data subject must either be made aware of, or informed of: the purpose of data processing; categories of third parties to whom the data might be transmitted

- Processing of personal data must have received the consent of the data subject or must meet one of the following conditions: compliance with any legal obligation to which BEDC is subject; the protection of the data subject's life; the performance of a public service mission entrusted to BEDC.

4.4 Confidentiality and Data Security

- Personal data is subject to data secrecy. It must be treated as confidential on a personal level and secured with suitable organizational and technical measures to prevent unauthorized access, illegal processing, or distribution, as well as accidental loss, modification, or destruction.

4.5 Deletion

- Personal data shall be retained in a form that allows the identification of the data subjects for a period no longer than is necessary for the purposes for which they are obtained and processed. There may be an indication of interests that merit protection or historical significance of this data in individual cases. If so, the data must remain on file until the interests that merit protection have been clarified legally, or the corporate archive has evaluated the data to determine whether it must be retained for historical purposes.

4.6 Factual Accuracy and Up-to-datedness of Data

- Personal data on file must be correct, complete, and if necessary, kept up to date. Suitable steps must be taken to ensure that inaccurate or incomplete data are deleted, corrected, supplemented, or updated.

5.0 RESPONSIBILITIES

Everyone who works for or with BEDC has some responsibility for ensuring data is collected, stored, and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection regulation. However, these people have key areas of responsibility:

a. **The Managing Director/Chief Executive Officer and Board of Directors**

are responsible for ensuring that BEDC meets its legal obligations.

b. The Data Protection Officer (DPO) is responsible for:

- Keep the executive management and board updated about data protection responsibilities, risks, and issues.
- Review all data protection procedures and related policies, in line with an agreed schedule.
- Arrange data protection training and advice for the people covered by this policy.
- Handle data protection questions from staff and anyone else covered by this policy.
- Deal with requests from individuals to see the data BEDC holds about them (also called 'subject access requests').
- Vet any contracts or agreements with third parties that may handle the company's sensitive data.
- Vet any data protection statements attached to communications such as emails and letters.
- Address any data protection queries from journalists or media outlets like newspapers.
- Where necessary, work with other staff members to ensure marketing initiatives abide by data protection principles.

c. The Chief Information Officer (CIO) is responsible to:

- Ensure all systems, services and equipment used for storing data meet acceptable security standards.
- Perform regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluate any third-party services the company is considering using to store or process data. For instance, cloud computing services.

6.0 GENERAL STAFF GUIDELINES

- The only employees able to access data covered by this policy should be those who need it to execute their job effectively.

- Data should not be shared informally. When access to confidential information is required, employees can request for it from their line managers.

- Employees should keep all data secure, by taking sensible precautions and following the guidelines below:

    1. In particular, strong passwords must be used, and they should never be shared.
    2. Personal data should not be disclosed to unauthorized people, either within the company or externally.
    3. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
    4. Employees should request help from their line manager or the data protection officer (DPO) if they are unsure about any aspect of data protection.

7.0 DATA STORAGE

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the Chief Information Officer (CIO).
When data is stored on paper, it should be kept in a secure place where unauthorized person(s) cannot access it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorized person(s) could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required.

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

- Data should be protected by strong passwords that are changed regularly and never shared with colleague(s).
- If data is stored on removable media (like a flash drive, CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers and should only be uploaded to approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

- All servers and computers containing data should be protected by approved security software and a firewall.

8.0 DATA USE

Personal data is of no value to BEDC unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft:

- When working with personal data, employees should ensure the screens of their computers are always locked when left unattended.
- Personal data should never be transferred outside of Nigeria without the consent of the data subject.

9.0 DATA ACCURACY

The law requires BEDC to take reasonable steps to ensure data is kept accurate and up to date.

The more important it is that the personal data is accurate, the greater the effort BEDC should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.
- Data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

10. SUBJECT ACCESS REQUEST

All individuals who are the subject of personal data held by BEDC are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

If an individual contacts the company requesting this information, this is called a subject access request (SAR).

Subject access requests from individuals should be made by email, addressed to the Data Protection Officer (DPO) through the designated/assigned email address.

Individuals will be charged N2,000.00 per subject access request. BEDC shall aim to provide the relevant data within 14 days.

BEDC shall always verify the identity of anyone making a subject access request before handing over any information.

11. DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the Nigerian Data Protection Regulation allows personal data to be disclosed to law enforcement agencies or court without the consent of the data subject.

Under these circumstances, BEDC will disclose requested data. However, BEDC shall ensure the request is legitimate, seeking assistance from the board and company's legal advisers where necessary.

12. PROVIDING INFORMATION

BEDC aims to ensure that individuals are aware that their data is being processed, and that they understand:

- How the data is being used
- How to exercise their rights

To these ends, the company has a privacy policy, which sets out how data relating to individuals are used by the company. Please, refer to BEDC's privacy policy on the corporate website.