DATA PROTECTION POLICY

(DOC. NO: AKD-ICT-POL-01)

DATA PROTECTION POLICY

Rev. No.	Issue Date	Prepared By	Reviewed by	Approved By
00	03-Jul-2023	Daniel Ugwu (ICT)	Chioma Omoruyi (QAQC)	Daniel Ugwu (ICT)

CHANGE(S)/AMENDMENT(S)

The change(s)/amendment(s) noted below have been made and approved by Management for issue.

Change/Amendment No.	Date	Page	Description of Change/ Amendment
00	03-Jul-2023	All Pages	First issue

DATA PROTECTION POLICY

DATA PROTECTION POLICY

1. INTRODUCTION

AKD Digital Solutions needs to gather and use certain information about individuals.
These can include customers, suppliers, business contacts, employees, and other people the organization has a relationship with or may need to contact.
This policy describes how this personal data must be collected, handled, and stored to meet the company's data protection standards — and to comply with the law.

2. Purpose of **AKD Data Protection Policy**

This data protection policy ensures AKD Digital Solutions

a) Complies with Nigeria Data Protection Regulation (NDPR) and follow best practice

b) Protects the rights of staff, customers and partners

c) Is open about how it stores and processes individuals' data by making its data protection policy available to the public

d) Protects itself from the risks of a data breach

The National Information Technology Development Agency (NITDA) Nigeria Data Protection Regulation (NDPR) setup by the NITDA Act of 2007 describes how organizations — including AKD Digital Solutions — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials

3. General objective OF THE Nigeria Data Protection regulation:

a) To safeguard the rights of natural persons in Nigeria to data privacy with respect to the processing of their personal data.

b) to foster safe conduct for transactions involving the exchange of

Personal Data.

c) to prevent manipulation of Personal Data

d) To ensure that Nigerian Businesses remain competitive in international trade through the safe guards afforded by a sound data protection regulation.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Nigeria Data Protection Regulation is underpinned by the following important principles.

4. Key Features of NDPR

a) Clarity of Privacy Policy: Any medium through which Personal Data is being collected or processed shall display a simple and conspicuous privacy policy that the class of Data Subject being targeted can understand

b) Lawful Processing: Personal data be obtained only for specific lawful purposes consented by the data subject.

c) Data Integrity and Storage Limitation: Be adequate, accurate and without prejudice to the dignity of human persons

d) Data Minimization: Not be held for any longer than necessary

e) Explicit consent: Processed in accordance with the explicit consent and rights of data subjects

f) Security of data: Data be protected in appropriate ways by data controllers

g) Prohibition of improper motives: No consent shall be sought, given or accepted in any circumstance that may engender propagation of atrocities, hate, child rights violation, criminal and anti-social acts

h) International Data transfer: Not be transferred outside the European Economic Area (EEA), unless by NITDA assessment that country or territory also ensures an adequate level of protection. Transfer activities are subject to the supervision of the Honorable Attorney General of the Federation.

5. Policy Scope

This policy applies to:

- The Head Office of AKD Digital Solutions
- All branch Offices of AKD Digital Solutions
- All Category of staff including volunteers of AKD Digital Solutions
- All contractors, suppliers, business partners and other people working on behalf of AKD Digital Solutions.
- All data that the company holds relating to identifiable individuals, even if that information technically falls outside of the Nigerian Data Protection Regulation 2019. This can include Names of individuals, Postal addresses, Email addresses, Telephone numbers.

6. Data protection risks

This policy helps to protect AKD Digital Solutions from some very real data security risks, including:

i) Breaches of confidentiality. For instance, information being given out inappropriately.

ii) Failing to offer choice. For instance, all individuals should be free to choose how the company uses data relating to them.

iii) Reputational damage. For instance, the company could suffer if hackers successfully gained access to sensitive data.

7. Responsibilities

Everyone who works for or with AKD Digital Solutions 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 principles.

However, these people have key areas of responsibility:

The CHAIRMAN/GCEO

The CHAIRMAN/GCEO is ultimately responsible for:

- Ensuring that AKD Digital Solutions meets its legal obligations.
- Keeping the board updated about data protection responsibilities, risks, and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

Executive Director, Corporate Service Unit (ED, CSU)

ED CSU is responsible:

- Approving any data protection statements attached to communications such as emails and letters.
- Handling data protection questions from staff and anyone else covered by this policy.
- Addressing any data protection queries from journalists or media outlets like newspapers.

- Dealing with requests from individuals to see the data AKD Digital Solutions holds about them.

Data Protection Officer (DPO): DPO is responsible for:

- Arranging data protection training and advice for the people covered by this policy
- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

8. General staff guidelines

a) The only people able to access data covered by this policy should be those who need it for their work.

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

c) AKD Digital Solutions will provide training to all employees to help them understand their responsibilities when handling data.

d) Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

e) Strong passwords must be used, and they should never be shared.

f) Personal data should not be disclosed to unauthorized people, either within the company or externally.

g) 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.

h) Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

These rules describe how and where data should be safely stored.

1) When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it.

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

3) When not required, the paper or files should be kept in a locked drawer or filing cabinet.

4) Employees should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.

5) Data printouts should be shredded and disposed of securely when no longer required.

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

7) Data should be protected by strong passwords that are changed regularly and never shared between employees.

8) If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.

9) Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing service.

10) Servers containing personal data should be sited in a secure location, away from general office space.

11) Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.

12) Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

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

9. Data storage

Personal data is of no value to AKD Digital Solutions 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.

a) Personal data should not be shared informally. It should never be sent by email, as this form of communication is not secure.

b) Data must be encrypted before being transferred electronically.

c) Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

10. Procedure for Data Breach Incident

Definition of Breach

A data breach is 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. Such incidents may be caused by:

- Accidental loss
- Theft
- Human error e.g., email containing personal data sent to the wrong person
- Equipment failure
- Damage e.g., fire, flood
- Malicious activity e.g., hacking

If a data security breach occurs, AKD Digital Solutions will respond to and manage the breach effectively by means of a 5-part process.

1. Reporting a Breach
2. Containment and Recovery
3. Assessing the Risks
4. Notification of Breaches
5. Evaluation and Response

Reporting a Breach

AKD Digital Solutions are to report breaches to appropriate authority within 72 hours after discovery through the help of Data Protection Officer (DPO).

Containment and Recovery

Once details of the breach are known, the DPO will liaise with relevant personnel to contain the effect of the breach. This may include personnel from ICT, Human Resources, AKD Digital Management Team, external suppliers. The DPO and the department

specialists will agree what action must be taken to limit the damage caused by the breach and if possible, restore any lost data e.g., backup on external hard disk. Priority actions may include password changes, disabling swipe access to secure areas within the buildings or searching for lost equipment.

Assessing the Risks

Once the breach has been contained, the DPO and department specialists will assess the risks associated with the loss of the data. Considerations will be given to the following points:

- Type of data e.g., hardcopy, electronic, personal data, sensitive data
- Nature of the loss e.g., theft, damage
- Has the data been encrypted
- What information does the data tell an unauthorised party who may now have access
- How many individuals are potentially affected by this loss
- What category of individuals are affected e.g., students, staff, suppliers
- What threat may be posed to these individuals e.g. financial loss, personal safety.

Notification of Breaches

Where data loss has been confirmed, AKD Digital Solutions is obliged to notify all parties affected by the breach. Notifying the individuals, the DPO and department specialists will establish the identities of individuals whose personal data has been compromised and agree on the correspondence to be sent to each subject.

The correspondence should include:

- How and when the breach occurred
- What data is involved
- Actions taken by the AKD Digital Solutions

- Nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- Name and contact details of the data protection officer or other contact point where more information can be obtained
- Describe the likely consequences of the personal data breach
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Evaluation and Response

While it is critical to contain and assess the risks of a breach, AKD Digital Solutions must evaluate events leading to the breach and the effectiveness of its response to it. While carrying out an evaluation the DPO will convene with department heads to seek measures AKD Digital Solutions should take to avoid a breach of a similar nature in the future. Considerations should be given to the following:

- Was the breach a result of inadequate policies or procedures
- Was the breach a result of inappropriate training
- Where are documents stored
- Who has access rights to what data
- Has this breach identified potential weaknesses in other areas
- Security of electronic information assets

11. Data accuracy

The law requires AKD Digital Solutions 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 AKD Digital Solutions 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.

i. Data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.

ii. Staff should take every opportunity to ensure data is updated. For instance, by confirming a customer's details when they call.

iii. AKD Digital Solutions will make it easy for data subjects to update the information it holds about them. For instance, via the company ERP HR Module.

iv. 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.

v. It is the marketing manager's responsibility to ensure marketing databases are checked against industry suppression files every six months.

12. Subject access requests

All individuals who are the subject of personal data held by AKD Digital Solutions are entitled to:

1. Ask what information the company holds about them and why.

2. Ask how to gain access to it.

3. informed how to keep it up to date.

4. Be informed how the company is meeting its data protection obligations.
   A subject access request is a request by an individual to the company requesting information relating to any or whole of his or her personal information.

Subject access requests from individuals should be made by email, addressed to the data controller at **i.akobo@pe-ng.com**. The data controller can supply a standard request form, if preferred although individuals do not have to use this.

Individuals will not be charged for an access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

13. Disclosing data for other reasons

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

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

14. Providing information

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

I. How the data is being used

II. How to exercise their right.

To these ends, the company has a privacy statement, setting out how data relating to individuals is used by the company.

This is available on request.