DATA PROTECTION POLICY

Nigeria Data Protection Regulation (NDPR) & NDPA Compliance

Document Reference: POL-NDPR-001 **Version:** 2.0 **Effective Date:** January 1, 2025 **Review Date:** January 1, 2026 **Classification:** Confidential

---

1. INTRODUCTION

This policy outlines our commitment to protecting personal data in compliance with Nigerian data protection legislation and regulations.

2. LEGAL FRAMEWORK

This policy is established in accordance with: - **Nigeria Data Protection Act (NDPA) 2023** - Primary legislation - **Nigeria Data Protection Regulation (NDPR) 2019** - NITDA's implementing regulation - **NDPR Implementation Framework 2020** - **Cybercrimes (Prohibition, Prevention, etc.) Act 2015** - **Constitution of the Federal Republic of Nigeria 1999** - Section 37 (Right to Privacy) - **Freedom of Information Act 2011** - **National Information Technology Development Agency (NITDA) Act 2007**

2.1 Regulatory Authority

The Nigeria Data Protection Commission (NDPC), established under Section 6 of NDPA 2023, is the primary regulator. Until NDPC is fully operational, NITDA continues to enforce NDPR.

3. PURPOSE

To ensure that: - Personal data is processed lawfully, fairly, and transparently - Data subjects' rights are protected under Nigerian law - The Company meets its obligations under NDPA and NDPR - Staff understand their responsibilities regarding data protection - Compliance with data audit and registration requirements

4. SCOPE

This policy applies to: - All personal data processed by the Company - All employees, contractors, and third parties with data access - All systems and processes involving personal data - Both electronic and manual records - Data processed within and outside Nigeria involving Nigerian data subjects

5. KEY DEFINITIONS

Term	Definition
Personal Data	Information relating to an identified or identifiable natural person
Data Subject	The individual whose personal data is being processed
Data Controller	Entity that determines purposes and means of processing
Data Processor	Entity that processes data on behalf of the controller

Term	Definition
Sensitive Data	Data revealing race, religion, health, biometrics, political opinions

5. DATA PROTECTION PRINCIPLES

5.1 Lawfulness, Fairness, and Transparency

- Process data only with valid legal basis
- Inform data subjects of processing activities
- Maintain clear privacy notices

5.2 Purpose Limitation

- Collect data for specified, explicit purposes
- Do not process data incompatibly with original purposes
- Document all processing purposes

5.3 Data Minimization

- Collect only necessary data
- Avoid excessive data collection
- Regularly review data held

5.4 Accuracy

- Keep personal data accurate and up-to-date
- Establish procedures for data correction
- Delete or correct inaccurate data promptly

5.5 Storage Limitation

- Retain data only as long as necessary
- Implement retention schedules
- Securely dispose of data when no longer needed

5.6 Integrity and Confidentiality

- Implement appropriate security measures
- Protect against unauthorized access
- Guard against accidental loss or damage

6. LAWFUL BASIS FOR PROCESSING

Processing is lawful only if based on: 1. **Consent** - Clear, specific, informed agreement 2. **Contract** - Necessary for contractual performance 3. **Legal Obligation** - Required by Nigerian law 4. **Vital Interests** - Protecting someone's life 5. **Public Interest** - Official authority functions 6. **Legitimate Interests** - Balanced against data subject rights

7. DATA SUBJECT RIGHTS

Individuals have the right to: - **Information** - Know how their data is used - **Access** - Obtain copies of their data - **Rectification** - Correct inaccurate data - **Erasure** - Request deletion of data - **Restriction** - Limit processing in certain cases - **Portability** - Receive data in usable format - **Objection** - Object to certain processing - **Automated Decisions** - Not be subject to solely automated decisions

Response Timeframes

- Acknowledge requests within 72 hours
- Complete requests within 30 days
- Extensions up to 60 days for complex requests

8. DATA SECURITY MEASURES

8.1 Technical Measures

- Encryption of sensitive data at rest and in transit
- Multi-factor authentication for system access
- Regular security patches and updates
- Firewall and intrusion detection systems
- Regular backup procedures

8.2 Organizational Measures

- Access controls based on role requirements
- Staff training on data protection
- Clean desk policy
- Secure disposal procedures
- Incident response procedures

9. DATA BREACH PROCEDURES

9.1 Definition

A data breach is any security incident that leads to accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data.

9.2 Response Steps

1. **Contain** - Stop the breach immediately
2. **Assess** - Determine scope and impact
3. **Notify** - Inform DPO within 24 hours
4. **Report** - Notify NITDA within 72 hours if required
5. **Inform** - Notify affected individuals if high risk
6. **Document** - Record all breach details
7. **Review** - Implement preventive measures

9.3 Reporting to NITDA

Breaches must be reported if likely to result in risk to rights and freedoms. Report via: https://nitda.gov.ng/nit/breach-notification/

10. INTERNATIONAL TRANSFERS

Personal data may only be transferred outside Nigeria if: - Adequate protection exists in destination country - Appropriate safeguards are implemented - Data subject has consented - Transfer is necessary for contract performance

11. TRAINING REQUIREMENTS

All staff must complete: - NDPR awareness training within 30 days of joining - Annual refresher training - Role-specific training for data handlers

12. DATA PROTECTION OFFICER

Contact Details: - Email: dpo@company.com - Phone: +234 XXX XXX XXXX - Office: Human Resources Department

14. DATA PROTECTION COMPLIANCE OFFICER (DPCO)

14.1 DPCO Registration

In accordance with NDPR Article 4.1(7), organizations processing personal data of more than 2,000 data subjects in any 12-month period must: - Appoint a Data Protection Compliance Officer - Register with NITDA/NDPC within 6 months of operation - Conduct annual Data Protection Audit - File annual compliance returns

14.2 Data Protection Audit

Annual audit must be conducted by a licensed Data Protection Compliance Organization (DPCO) and filed with NITDA/NDPC.

15. COMPLIANCE AND PENALTIES

15.1 NDPA 2023 Penalties

As per Part IX of the NDPA 2023:

Offence	Penalty
Processing without lawful basis	Up to ₦10 million or 2% of annual turnover
Failure to implement security measures	Up to ₦10 million or 2% of annual turnover
Failure to notify data breach	Up to ₦5 million
Obstruction of NDPC investigation	Up to ₦2 million
Failure to register as DPCO	Up to ₦5 million

15.2 Criminal Liability

Under the Cybercrimes Act 2015, unauthorized access to computer systems or data may result in imprisonment.

15.3 Civil Liability

Data subjects may seek compensation for damages suffered due to non-compliance.

15.4 Employee Consequences

Employees who breach this policy may face: - Disciplinary action up to termination - Personal liability for willful misconduct - Report to relevant authorities

16. REGULATORY CONTACTS

- **NITDA:** www.nitda.gov.ng
- **NDPC:** www.ndpc.gov.ng
- **Breach Notification Portal:** https://nitda.gov.ng/nit/breach-notification/
- **DPCO Registration:** https://nitda.gov.ng/nit/data-protection/

17. POLICY REVIEW

This policy will be reviewed: - Annually - Following significant data breaches - When regulations change - After organizational changes

---

Data Protection Officer: [Name] **Approved by:** Managing Director **Date:** December 15, 2024

Employees must acknowledge this policy within 14 days of receipt.