NDPA Audit Framework for Greenacres Microfinance Bank

This document outlines a comprehensive audit framework to assess **Greenacres** Microfinance Bank's compliance with the Nigeria Data Protection Act (NDPA) 2023 and its General Application and Implementation Directive (GAID) 2025.

1. Executive Summary

- **Purpose:** To provide an independent assessment of the Microfinance Bank's adherence to the NDPA and GAID.
- **Scope:** All personal data processing activities, systems, policies, procedures, and personnel involved in handling customer, employee, vendor, and other third-party personal data.
- **Key Findings (to be completed after audit):** Summary of compliance status, identified gaps, and high-level recommendations.

2. Introduction to NDPA Compliance for Greenacres Microfinance Bank

- **Legal Basis:** NDPA 2023 and GAID 2025.
- **Classification:** Microfinance banks are typically classified as Data Controllers of Major Importance (DCMI) due to the nature and volume of personal data processed (especially sensitive financial data). This classification imposes specific obligations, including mandatory annual audits.
- **Penalties for Non-Compliance:** Outline the potential fines (up to N10 million or 2% of annual gross revenue, whichever is higher, for DCMIs) and other sanctions (e.g., public listing on non-compliance register).
- **Role of Data Protection Compliance Organization (DPCO):** Emphasize that the audit must be conducted by a licensed DPCO and the annual Compliance Audit Report (CAR) filed with the Nigeria Data Protection Commission (NDPC).

3. Audit Methodology

- **Phase 1: Planning & Scoping:**
    - Define audit objectives and scope.
    - Identify relevant departments and stakeholders (e.g., IT, Legal, Operations, HR, Marketing, Customer Service).
    - Request relevant documentation (policies, procedures, contracts, data inventories).
- **Phase 2: Data Collection & Analysis:**
    - Interviews with key personnel.
    - Review of documentation.
    - Technical assessments (e.g., security controls, system configurations).

    - Sample testing of processes.
- **Phase 3: Reporting & Recommendations:**
    - Analysis of findings against NDPA requirements.
    - Identification of gaps and risks.
    - Development of actionable recommendations.
    - Presentation of the Compliance Audit Report (CAR).

4. Audit Areas and Checklist

This section details the specific areas to be audited, along with key considerations and evidence.

4.1. Data Governance and Accountability

- **NDPA Requirement:** Section 29 (Accountability), Article 10 (CAR), Article 11 (DPO).
- **Key Considerations:**
    - **Appointment of Data Protection Officer (DPO):**
        - Is a qualified DPO appointed?
        - Does the DPO have direct access to senior management and sufficient resources?
        - Is the DPO's role and responsibilities clearly defined and documented?
        - Is the DPO independent and free from conflicts of interest?
    - **Data Protection Policies & Procedures:**
        - Are comprehensive data protection policies in place (e.g., Privacy Policy, Information Security Policy, Data Retention Policy, Data Breach Management Policy, DPIA Policy)?
        - Are these policies regularly reviewed and updated (e.g., annually, or upon significant changes)?
        - Are policies easily accessible to relevant staff and data subjects?
    - **Record of Processing Activities (ROPA):**
        - Does the bank maintain a detailed and up-to-date ROPA (data inventory/asset register) as per Section 34 of the NDPA?
        - Does the ROPA include: categories of personal data, purposes of processing, categories of data subjects, recipients, retention periods, security measures, and cross-border transfers?
    - **Management Commitment:**

        - Is there clear evidence of C-Suite and Board awareness and commitment to NDPA compliance?
        - Are regular updates on NDPA compliance provided to management?

4.2. Lawfulness, Fairness, and Transparency

- **NDPA Requirement:** Section 24(1)(a) (Lawfulness, Fairness, Transparency), Section 25 (Lawful Basis), Section 30 (Privacy Notice).
- **Key Considerations:**
    - **Lawful Basis for Processing:**
        - For every processing activity, is a valid lawful basis identified and documented (consent, contract, legal obligation, vital interest, public interest, legitimate interest)?
        - For consent-based processing, is consent freely given, specific, informed, and unambiguous? (e.g., separate checkboxes for different purposes, clear language).
        - Is there a clear mechanism for data subjects to withdraw consent?
    - **Privacy Notice/Policy:**
        - Is a comprehensive and easily accessible Privacy Policy published (e.g., on the bank's website, mobile app, and available in branches)?
        - Does it clearly inform data subjects about: identity of controller, DPO contact, purposes of processing, lawful basis, categories of data collected, recipients, retention periods, data subject rights, and complaint mechanisms?
        - Is it written in clear, plain language?
    - **Transparency in Data Collection:**
        - Are data subjects informed at the point of data collection about the purpose and lawful basis? (e.g., on forms, digital interfaces).

4.3. Purpose Limitation and Data Minimization

- **NDPA Requirement:** Section 24(1)(b) (Purpose Limitation), Section 24(1)(c) (Data Minimization).
- **Key Considerations:**
    - **Purpose Limitation:**
        - Is personal data collected only for specified, explicit, and legitimate purposes?
        - Is there a process to prevent further processing incompatible with original purposes without new consent or lawful basis?
    - **Data Minimization:**

        - Is only adequate, relevant, and necessary personal data collected for the stated purposes?
        - Are processes in place to avoid excessive or irrelevant data collection?
        - Is anonymization or pseudonymization considered where feasible?

4.4. Data Accuracy and Storage Limitation

- **NDPA Requirement:** Section 24(1)(d) (Accuracy), Section 24(1)(e) (Storage Limitation).
- **Key Considerations:**
    - **Data Accuracy:**
        - Are measures in place to ensure personal data is accurate and kept up-to-date? (e.g., data validation, regular reviews, mechanisms for data subjects to request rectification).
        - Is there a process to correct or erase inaccurate data promptly?
    - **Storage Limitation/Retention:**
        - Are clear data retention policies established for different categories of personal data?
        - Is personal data retained only for as long as necessary for the purposes for which it was collected or for legal/regulatory obligations?
        - Are mechanisms in place for secure disposal or anonymization of data after retention periods expire?

4.5. Integrity and Confidentiality (Security Measures)

- **NDPA Requirement:** Section 24(1)(f) (Integrity and Confidentiality), Section 33 (Security Measures), Section 35 (Data Breach Notification).
- **Key Considerations:**
    - **Technical and Organizational Security Measures:**
        - Are appropriate technical controls implemented (e.g., encryption, access controls, firewalls, intrusion detection systems, antivirus, regular vulnerability assessments, penetration testing)?
        - Are appropriate organizational measures in place (e.g., staff training, clear roles and responsibilities, incident response plan)?
        - Is there a robust access management system (least privilege, need-to-know basis)?
        - Are sensitive personal data (e.g., BVN, account numbers, biometric data) subject to enhanced security measures?

- **Data Breach Management:**
    - Is a comprehensive Data Breach Notification Procedure in place?
    - Does it include steps for detection, containment, assessment, notification (to NDPC and affected data subjects within 72 hours where applicable), and remediation?
    - Is an internal breach register maintained?
- **Physical Security:**
    - Are physical access controls in place for data storage facilities and IT infrastructure?
- **Vendor/Third-Party Security:**
    - Are due diligence processes in place for assessing the data protection practices of third-party vendors/processors?
    - Are Data Processing Agreements (DPAs) in place with all third-party processors, clearly outlining responsibilities and security obligations?

4.6. Data Subject Rights

- **NDPA Requirement:** Sections 37-41 (Data Subject Rights).
- **Key Considerations:**
    - **Mechanisms for Exercising Rights:**
        - Are clear and easily accessible procedures in place for data subjects to exercise their rights (e.g., Right to be Informed, Access, Rectification, Erasure/Right to be Forgotten, Restriction of Processing, Objection, Data Portability, Rights related to Automated Decision Making)?
        - Is there a dedicated contact point (e.g., DPO) for data subject requests?
    - **Response Time:**
        - Are requests from data subjects responded to within the stipulated timeframe (usually 30 days)?
    - **Verification:**
        - Are appropriate identity verification procedures in place to ensure requests are legitimate?

4.7. Cross-Border Data Transfer

- **NDPA Requirement:** Section 43 (Cross-Border Transfer).
- **Key Considerations:**

- **Adequacy Decision:**
    - Is personal data transferred outside Nigeria only to countries with an adequate level of data protection as determined by the NDPC?
- **Appropriate Safeguards:**
    - If not to an adequate country, are appropriate safeguards in place (e.g., Standard Contractual Clauses, Binding Corporate Rules, explicit consent of the data subject)?
- **Documentation:**
    - Are all cross-border data transfers and the legal basis/safeguards for such transfers properly documented?

4.8. Staff Training and Awareness

- **NDPA Requirement:** Section 36 (Training and Awareness).
- **Key Considerations:**
    - **Regular Training:**
        - Is mandatory data protection and privacy training provided to all employees (especially those handling personal data) on an ongoing basis?
        - Does the training cover NDPA principles, bank policies, data subject rights, and breach reporting procedures?
    - **Awareness Programs:**
        - Are regular awareness campaigns conducted (e.g., emails, posters, internal memos) to reinforce data protection best practices?
    - **Documentation of Training:**
        - Are records of all training sessions and employee participation maintained?

5. Audit Findings and Recommendations

- **Detailed Findings:** For each audit area, list specific findings, including areas of compliance and non-compliance.
- **Risk Assessment:** Assess the severity and likelihood of risks associated with each non-compliance.
- **Recommendations:** Provide clear, actionable recommendations for addressing identified gaps and improving data protection posture. Prioritize recommendations based on risk level.
- **Action Plan (Template):** Include a template for the bank to develop an action plan, assigning responsibilities and deadlines for each recommendation.
-

6. Conclusion

- Overall assessment of the bank's NDPA compliance maturity.
- Emphasis on continuous monitoring and improvement.
- Confirmation of the DPCO's role in ongoing compliance support.

Disclaimer: This framework provides a general guide for an NDPA audit. A licensed Data Protection Compliance Organization (DPCO) in Nigeria must conduct the actual audit, as they possess the specific expertise and are mandated by the NDPC to perform and file the Compliance Audit Report. This document does not constitute legal advice.