Nigeria Data Protection Compliance Process

Effective from September 2023 to present.

Adamawa State Government ICT Policies and Procedures
adamawastate.gov.ng

Office of Secretary of the State Government
Adamawa State Secretariat

Purpose of Policy	The purpose of this process is to establish a systematic approach to NDPR compliance within Adamawa State government and its agencies, safeguarding personal data, and fostering a culture of data protection.
Internal Services Involved	Office of the SSG/ASITDA
Related Policies and Procedures	a. ADSG ICT Policy (ADSG Digital Transformation Agenda and Roadmap) b. ADSG Email Use Policy c. ADSG Compliance Process with NDPA, 2023
Enquiries To:	ICT, Strategy and Policy Office SAICT@adamawastate.gov.ng Office of the SSG, Adamawa State Secretariat Adamawa State Government Nigeria

Version	v.01
Owner	Office of the SSG
Date Approved	
Review Date	20 September, 2023
Reviewer	SSG

Contents

A. Introduction

This document outlines the Nigeria Data Protection Regulation (NDPR) compliance process for Adamawa State, detailing the steps and actions required to ensure adherence to data protection regulations.

B. Purpose

The purpose of this process is to establish a systematic approach to NDPR compliance within Adamawa State government and its agencies, safeguarding personal data, and fostering a culture of data protection.

C. Scope of Applicability

This compliance process applies to all government entities, departments, and agencies operating within Adamawa State, handling personal data in compliance with NDPR.

D. Definitions

- **Data Protection Officer (DPO):** An appointed individual responsible for ensuring compliance with data protection regulations.
- **Privacy Impact Assessment (PIA):** An assessment conducted to evaluate the impact of data processing activities on privacy.
- **Data Subject Consent:** Consent obtained from individuals for the processing of their personal data.
- **Data Breach Response Plan:** A plan outlining procedures for handling and reporting data breaches.
- **Vendor Management:** The process of assessing and ensuring data protection compliance of third-party vendors.
- **Data Processing:** Any operation performed on personal data, including collection, storage, and use.
- **Regulatory Reporting:** The submission of data protection activities to relevant authorities as required by NDPR.

E. Process Statements

- Establish awareness and understanding of NDPR requirements among stakeholders.
- Designate a Data Protection Officer (DPO) to oversee compliance efforts.
- Identify, document, and map all personal data processing activities.
- Conduct Privacy Impact Assessments (PIAs) to mitigate privacy risks.
- Develop and implement a Data Protection Policy aligned with NDPR.
- Establish processes for managing data subject consent.
- Implement data security measures to protect personal data.
- Create a Data Breach Response Plan for effective incident management.
- Assess and ensure data protection compliance of third-party vendors.
- Provide data protection training to employees and stakeholders.
- Conduct regular audits and assessments of data protection measures.
- Maintain comprehensive documentation for compliance evidence.
- Continuously review and improve the data protection compliance process.
- Fulfill regulatory reporting obligations.
- Enforce compliance measures and initiate remediation for non-compliance.
- Communicate data protection practices and policies to the public, building trust and transparency.

F. Prepare for Data Security

- Outline measures for data inventory, mapping, and classification.
- Define data retention policies.
- Ensure secure data disposal procedures.
- Implement access controls and encryption where necessary.

G. Process Steps

Step 1: Data Protection Policy Establishment

- Description of the Step: Develop and establish comprehensive data protection policies in accordance with NDPR.
- Responsible Party: Data Protection Officer (DPO).
- Inputs: NDPR regulations, legal consultation.
- Actions:
  - Review NDPR requirements.
  - Draft data protection policies.
  - Seek legal review and approval.
  - Communicate policies to stakeholders.
- Resources: Legal/Data Protection expertise.
- Outputs: Established data protection policies.

Step 2: Data Inventory and Classification

- Description of the Step: Identify and classify all data collected and processed.
- Responsible Party: Data Owners.
- Inputs: Data inventories, data processing records.
- Actions:
  - Create data inventories.
  - Classify data based on sensitivity.
  - Document data flows.
- Resources: Data inventory tools.
- Outputs: Data inventories and classifications.

Step 3: Data Protection Impact Assessment (DPIA)

- Description: Conduct a DPIA to assess and mitigate data protection risks associated with new or existing data processing activities.
- Responsibility: Data Protection Officer (DPO) and relevant department heads.
- Expected Inputs: Information about data processing activities, data flow diagrams, data protection policies.
- Actions:
  - Identify data processing activities.
  - Assess data protection risks.
  - Implement measures to mitigate risks.
- Resources: DPIA templates, data flow analysis tools.
- Expected Outputs: Completed DPIA reports, risk mitigation plans.

Step 4: Data Subject Rights Management

- Description: Establish procedures for handling data subject rights requests, including access, rectification, erasure, and portability.
- Responsibility: Data Protection Officer (DPO) and relevant department heads.
- Expected Inputs: Data subject rights requests.
- Actions:
  - Verify the identity of the data subject.
  - Process the request within the legal timeframe.
  - Provide requested information or actions.
- Resources: Data subject request forms, request tracking system.
- Expected Outputs: Processed data subject rights requests.

Step 5: Data Breach Response

- Description: Develop and implement a data breach response plan to address and report data breaches promptly.
- Responsibility: Data Protection Officer (DPO) and relevant department heads.
- Expected Inputs: Identification of a data breach.
- Actions:
  - Investigate the breach to determine its scope and impact.
  - Notify relevant authorities and data subjects as required by law.
  - Take corrective actions to prevent future breaches.
- Resources: Data breach response plan, incident reporting system.
- Expected Outputs: Data breach reports, documented corrective actions.

Step 6: Data Protection Training and Awareness

- Description: Provide data protection training to employees and raise awareness about data protection principles.
- Responsibility: Human Resources (HR) and Data Protection Officer (DPO).
- Expected Inputs: Training materials and schedules.
- Actions:
  - Develop training programs on data protection.
  - Conduct training sessions for employees.
  - Promote data protection awareness campaigns.
- Resources: Training materials, awareness materials.
- Expected Outputs: Trained employees, increased data protection awareness.

Step 7: Ongoing Compliance Monitoring

- Description: Establish continuous monitoring processes to ensure ongoing compliance with data protection regulations.
- Responsibility: Data Protection Officer (DPO) and Compliance Team.

- Expected Inputs: Compliance reports, audit findings.
- Actions:
  - Regularly review data protection policies and procedures.
  - Conduct compliance audits and assessments.
  - Address non-compliance issues promptly.
- Resources: Compliance monitoring tools, audit checklists.
- Expected Outputs: Compliance reports, documented corrective actions.

Related References
Following documents/links may be relevant to this policy.

Related Policies and Procedures	a. ADSG ICT Policy (ADSG Digital Transformation Agenda and Roadmap) b. ADSG Email Use Policy c. ADSG Compliance Process with NDPA, 2023

This process provides a comprehensive framework for NDPR compliance within Adamawa State, guiding government entities in safeguarding personal data and upholding data protection standards.