THE NIGERIAN SECURITY PRINTING AND MINTING PLC

DATA PROTECTION POLICY

PROCEDURE: DATA PROTECTION POLICY
DEPARTMENT: RISK MANAGEMENT
DIRECTORATE: CORPORATE SERVICES

DOCUMENT CONTROL

	DESIGNATION	NAME	SIGNATURE	DATE
Policy Owner(s):	Data Protection Officer	Chika Ikelionwu		
Authorized By:	Head, Risk Management	Samual Keffas		
Approved By:	Executive Committee	Exco		

REVISION TIMETABLE

REVISION	DESCRIPTION	DATE
1	Date Created	July, 2022
2	Version 1.0	July, 2023

Table of Contents

1. Introduction

Nigerian Security Printing and Minting Plc (NSPM) is dedicated to ensuring the privacy and security of personal data that it collects, stores, and processes, in line with applicable data protection laws and industry best practices. This Data Protection Policy details how NSPM safeguards personal data, outlines the roles and responsibilities related to data protection, and ensures adherence to the Nigerian Data Protection Act (NDPA) along with other relevant data protection laws.

The policy outlines the principles, responsibilities, and procedures for processing and protecting data within NSPM, ensuring that data confidentiality, integrity, and availability are always maintained.

2. Purpose of the Policy

This policy aims to:

- Ensure compliance with the Nigerian Data Protection Act (NDPA) and other relevant laws.
- Protect the rights of individuals whose personal data is processed by NSPM.
- Clearly define roles and responsibilities regarding data protection within NSPM.
- Establish secure procedures for handling personal data.
- Foster a culture of data protection and privacy throughout the organization.
- Encourage transparency and accountability in NSPM's data processing activities.
- Protect against data breaches and ensure swift action in the event of a data protection issue.

3. Scope

This policy applies to:

- All personal data processed by NSPM, both in manual and electronic form.
- All employees, contractors, consultants, temporary staff, and third-party service providers who have access to personal data held by NSPM.
- All departments, business units, and operations of NSPM.
- Both manual and electronic records that contain personal or sensitive data.

4. **Key Definitions**

• **Personal Data**: Any information that relates to an identified or identifiable individual, such as name, address, email, phone number, or identification number.

•**Sensitive Data**: This refers to personal information that reveals an individual's racial or ethnic background, political views, religious beliefs, health information, trade union membership, or sexual orientation.

• **Data Processing:** This encompasses any action taken on data, including its collection, storage, retrieval, modification, transfer, or deletion.

• **Data Subject:** The person to whom the personal data relates (for example, employees, customers, vendors).

• **Data Controller**: NSPM, which is the organization responsible for deciding the purposes and methods of processing personal data

• **Data Processor**: Any external party that processes personal data on behalf of NSPM.

5. Data Protection Principles

NSPM adheres to the following principles, as stipulated in the NDPA and international best practices:

1. **Lawful, Fair, and Transparent Processing**: Personal data will be processed in a lawful, fair, and transparent manner.
2. **Purpose Limitation**: Personal data will be collected for specific, legitimate purposes and will not be processed in ways that are incompatible with those purposes.
3. **Data Minimization**: Only personal data that is adequate, relevant, and necessary for the intended processing will be collected.
4. **Accuracy**: Personal data will be maintained accurately and updated as necessary
5. **Storage Limitation**: Personal data will not be retained longer than necessary for the purposes for which it was collected.
6. **Integrity and Confidentiality**: Personal data will be processed in a way that ensures appropriate security, integrity, and confidentiality.
7. **Accountability**: NSPM will be responsible for demonstrating adherence to these principles.

6. Roles and Responsibilities

6.1 Data Protection Officer (DPO)

NSPM appoints a **Data Protection Officer** (DPO), responsible for overseeing data protection activities. The DPO's responsibilities include:

1. Monitoring compliance with data protection laws.
2. Providing advice and guidance on data protection matters.
3. Conducting data protection impact assessments (DPIAs).
4. Acting as the point of contact for data subjects and supervisory authorities.
5. Ensuring staff are trained on data protection principles.
6. Coordinating responses to data breaches and incidents.

6.2 Employees

1. All employees of NSPM are responsible for:
2. Ensuring that personal data is processed in compliance with this policy.
3. Reporting any data breaches, risks, or concerns to the DPO.
4. Safeguarding data from unauthorized access, alteration, or destruction.
5. Participating in regular data protection training sessions.

6.3 Third-Party Service Providers

Third-party service providers with access to NSPM's personal data must comply with this policy. NSPM ensures that appropriate contracts and data protection agreements are in place with third parties to safeguard data security and privacy.

7. Types of Personal Data Processed

NSPM collects and processes the following types of personal data:

1. **Employee Data**: Names, contact details, job titles, salary details, performance reviews, tax information.
2. **Customer Data**: Names, contact information, transaction history, financial information.
3. **Vendor Data**: Business details, contact information, payment details.
4. **Visitor Data**: Names, contact details, identification information.
5. **Government Data**: Data collected for compliance with legal and regulatory requirements.

8. Data Collection, Processing, and Use

1. Personal data shall only be collected for specified, legitimate business purposes, such as for employee management, customer service, regulatory compliance, or financial transactions.
2. Data shall not be processed beyond the scope of the purpose for which it was collected, unless explicitly authorized by the data subject or required by law.
3. NSPM will ensure that data collection is conducted through lawful means, and data subjects will be informed about the purposes of data collection.

9. Data Security Measures

NSPM is dedicated to safeguarding the confidentiality, integrity, and availability of personal data by implementing appropriate security measures, which include:

1. **Access Control**: Access to personal data will be restricted to authorized personnel only, based on their roles and responsibilities.
2. **Encryption**: Personal data will be encrypted during transmission and while stored, to prevent unauthorized access.

3. **Firewalls and Antivirus Software**: NSPM will employ advanced security measures such as firewalls, antivirus software, and intrusion detection systems to protect personal data.
4. **Backup and Recovery**: Regular backups of personal data will be conducted, and disaster recovery plans will be established to restore data in the event of an incident.

10. Data Breach Management

In the event of a data breach, NSPM will:

a. **Notify the Data Protection Officer (DPO)** immediately.
b. **Evaluate the breach** to decide if it needs to be reported to the **National Information Technology Development Agency (NITDA)** and to affected individuals within 72 hours of discovery, in accordance with the NDPA.
c. **Implement corrective measures** to contain and lessen the impact of the breach
d. **Document the breach** and the actions taken in the data breach log for future reference.
e. Keep an **incident response plan always updated** to handle data breaches effectively.

11. Monitoring and Compliance

NSPM will perform regular audits and assessments to ensure adherence to this policy and relevant data protection laws. The DPO will supervise the auditing process and ensure that necessary corrective actions are taken when required.

12. Data Subject Rights

NSPM respects the rights of individuals in relation to their personal data. These rights include:

a. **Right to Access**: Data subjects have the right to request access to their personal data held by NSPM.
b. **Right to Rectification**: Data subjects can request corrections to inaccurate or incomplete personal data.
c. **Right to Erasure**: Data subjects have the right to request the deletion of their personal data when it is no longer necessary for processing.
d. **Right to Restrict Processing**: Data subjects can request the restriction of processing under certain conditions.
e. **Right to Object**: Data subjects have the right to object to processing of their data under specific circumstances.
f. **Right to Data Portability**: Data subjects can request a copy of their data in a structured, commonly used format to transfer to another data controller.

13. Data Retention and Disposal

NSPM will keep personal data only for as long as it is necessary for the purposes for which it was collected. Once this period has elapsed, personal data will be securely disposed of to ensure it cannot be reconstructed or retrieved.

Data Retention Periods:

a. **Employee Data**: Kept for the duration of employment and for a specified period (7years for now) afterward, in accordance with legal and regulatory requirements.
b. **Customer Data**: Maintained for as long as the customer relationship is active, and as required for compliance with financial and tax laws.
c. **Financial Data**: Held for the minimum duration mandated by tax and financial regulations.

14. Training and Awareness

NSPM will offer regular data protection training to all employees, covering:

a. The significance of safeguarding personal data.
b. Legal obligations and best practices for data management
c. Identifying and reporting potential data breaches.
d. Privacy policies and internal procedures.

Training will be compulsory for employees who handle personal data and will be updated regularly to reflect changes in laws and regulations.

15. Compliance with Applicable Laws

NSPM will adhere to all relevant data protection laws and regulations, including:

Nigerian Data Protection Act (NDPA).

General Data Protection Regulation (GDPR) (if applicable).

ISO/IEC 27001: Information security management standards that include provisions for protecting personal data.

ISO/IEC 27701: A privacy extension to ISO/IEC 27001 that provides guidelines for managing personal data in a privacy-conscious manner.

NIST Privacy Framework: A framework for improving privacy risk management, aligned with NIST's cybersecurity framework

Local regulatory requirements from the Central Bank of Nigeria (CBN), the National Information Technology Development Agency (NITDA), and other relevant authorities.

16. Policy Review and Updates

This Data Protection Policy will be reviewed at least once a year, or more frequently if there are major changes to data protection laws, regulations, or NSPM's business operations. Any updates to this policy will be shared with all relevant stakeholders.

17. References

- Information Security Policy
- Privacy Policy
- Access Control Policy
- Data retention and Disposal Policy
- Risk Management Policy
- Data Classification and Labelling Policy

18. Approval and Acknowledgment

The undersigned acknowledges that they have read and understood the Data Protection Policy and agree to comply with its terms and conditions.

Samuel Keffas
Risk Manager

Date

Chika Ikelionwu
Data Protection Officer
Date