



**MRS OIL NIGERIA PLC
PRIVACY COMPLIANCE POLICY**

This Policy is issued pursuant to the Nigerian Data Protection Regulation, 2019 and International Best Practices on Data Protection.

| |
|--|
| Review Frequency This document is reviewed biennially. |
| Document Ref.: MRS PCP |
| Version Number: V. No. 1 |
| Document Author: Mr. Olatunji Sanusi Designation: I.T Manager |
| Document Owner: Designation: Data Protection Officer |

MRS Oil Nigeria Plc's Record of Change to the Data Compliance Policy

MRS Oil Nigeria Plc. ("the Company") records planned updates under this section. The version number, author's name and date, approver's name and date, change type (i.e., high-level descriptor such as: 'Contact List Updates'), and a brief summary of the changes to the plan should be provided in the appropriate columns. For reviews that did not result in any updates, record 'No Updates' in the 'Summary of Changes' column.

| Version | Author (Name, & Date) | Approver (Name, & Date) | Change type | Summary of Changes |
|---------|-----------------------|-------------------------|---------------|------------------------------------|
| 1.0 | | | Plan Creation | Created the Incident Response Plan |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Contents

- 1. INTRODUCTION4**
- 2. DEFINITION4**
- 3. ACCOUNTABILITY4**
- 4. ASSESSMENT AND RECORDS OF PROCESSING ACTIVITIES4**
- 5. CONFIDENTIALITY OF PERSONAL DATA4**
- 6. EMPLOYEE TRAINING AND AWARENESS5**
- 7. SUPPLIER/VENDOR COMPLIANCE PROGRAM.....5**
- 8. COMPLIANCE MONITORING5**
- 9. DATA PROTECTION IMPACT ASSESSMENT (DPIA).....5**
- 10. THE RESPONSIBILITIES OF THE COMPANY AS A DATA CONTROLLER AND/OR PROCESSOR6**
- 11. NOTIFICATION OF SECURITY AND DATA BREACH6**
- 12. SUB PROCESSING – CROSS BORDER DATA TRANSFER7**
- 13. PROCESSING DATA OUTSIDE NIGERIA7**
- 14. POLICY REVIEW7**

1. INTRODUCTION

This Data Privacy Compliance Program is designed to promote and implement the Company's policies for the protection of privacy of any personal data controlled or processed by the Company or on behalf of our business partners.

2. DEFINITION

- a. **Data Controller** means a person, Company, or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body);
- b. **Data Processor** means a person who processes data on behalf of a Data Controller. A Data Controller decides the purpose and process to be followed to process the data, while Data Processors holds and processes data, but do not have any responsibility or control over that data;
- c. **DPO** means Data Protection Officer;
- d. **DPIA** means Data Protection Impact Assessment;
- e. **NITDA** means the National Information Technology Development Agency;
- f. **NDPR** means Nigerian Data Protection Regulation, 2019;
- g. **The Company** means MRS Oil Nigeria Plc.;
- h. **The Customer** means any third party the Company has a business relationship with.

3. ACCOUNTABILITY

The DPO is responsible for compliance and the supervision of the implementation of the Nigerian Data Protection Regulation ("NDPR") by the Company in its operations. As part of the supervisory role, the DPO:

- a. Maintains a written record for processing activities carried out by the Company;
- b. Carries out a Data Protection Impact Assessment (DPIA), where necessary;
- c. Notifies Management of any personal data breach without delays.

For any information, you may contact the Data Protection Officer on inquiries@mrsholdings.com.

4. ASSESSMENT AND RECORDS OF PROCESSING ACTIVITIES

There is a periodic review of the Company's Data Protection Policies, which includes the entire process of collection, usage, storage and disposal of personal data of every Data Subject(s). After each review, an update to the policies, standards, governance and documentation is published on the Company's website and shared electronically with all stakeholders.

The Company ensures that during any update, only the minimum amount of necessary personal data is processed. Records of processing activities is maintained by the Company and it contains all information required by the Regulation which would be available to Data Subjects upon request. This information include the purpose for the processing, categories involved, the time limits, general description of technical and organizational security measures and the transfer of personal data to third party organizations or country.

5. CONFIDENTIALITY OF PERSONAL DATA

The Company understands the need to protect information, including personal information made available by employees in the performance of their duties. The Company has a duty to preserve

and protect confidential or restricted information. All employees, including employees contracted by third party organizations on behalf of the Company are subjected to confidentiality requirements through a specific confidentiality clause in the Employment or Engagement Contract.

6. EMPLOYEE TRAINING AND AWARENESS

There is periodic training on data privacy and security to keep employees informed of the Company's policies and procedures or any regulatory changes to the Data Protection Policies and Regulation.

All business partners or stakeholders of the Company commit to train it employees on Data Protection requirements and Policies.

7. SUPPLIER/VENDOR COMPLIANCE PROGRAM

The Company periodically reviews supplier/vendor contracts to ensure that the supply chain process is compliant with data protection requirements. A Data Protection Impact Assessment (DPIA) is carried out at intervals as part of the compliance program.

8. COMPLIANCE MONITORING

The Company keeps pace with changes in the laws and regulations in force. Changes that significantly affects the level of protection of processing conditions are promptly communicated to relevant stakeholders. This gives the stakeholder an opportunity to either object the change or terminate the contract before modifications are made. An example of such changes are intended changes on the addition or replacement of subcontractors. Such changes are communicated to the existing subcontractor, before the data is sent to the new subcontractor.

The Internal Audit Department of the Company in conjunction with the DPO, would conduct audits at intervals to verify the compliance status of the Company.

9. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The Company conducts a Data Protection Impact Assessment when specific risks occur that affects the rights and freedoms of data subjects. The Assessment is carried out in accordance with International Standard Guidelines for DPIA and NDPR.

A review of the DPIA and the processing procedure is carried out at intervals, when there is a change in the risk posed by processing the data, and/or when using new technologies and data processing is likely to result in a risk to the Data Subjects.

The Board of Directors of the Company sign the DPIA and customers' cooperation are required for a seamless assessment. When the Company acts as the Data Processor of customer's personal data, the Company would request for transparent information from its Customers. This is to determine if DPIA should be conducted and if specific technical and organizational security measures should be implemented, prior to processing the personal data.

Where the outcome of the DPIA is such that the risk cannot be mitigated, reduced or eliminated, the Data Controller and Processor would consider whether to reject the risk or not. High level risks identified by the DPIA may be reported to NITDA, for its review on the compliance level of the intended processing operations in line with the Regulation.

10. THE RESPONSIBILITIES OF THE COMPANY AS A DATA CONTROLLER AND/OR PROCESSOR

As a marketer of petroleum products, the Company process personal data in its capacity as a Controller for its operational use alone. The information collected is limited to the business contact details of the Customer for the purpose of contract administration and marketing. Based on the responsibilities of the Controller, the Company processes personal data with the principles of purpose limitation, data minimization, specific storage period, data quality, data protection by design and default, legal basis for processing, processing of special categories of personal data, measure to ensure data security and specific requirements for personal data transfer outside Nigeria.

We ensure lawful, fair and transparent processing of individuals' personal data and the Data Protection Policy of the Company provides information on the rights, rules and safeguards in relation to the processing of personal data, which is communicated to all stakeholders (Data Subjects) via the Company's website or email.

The Company maintains a Data Retention Policy, which provides a timeframe for the collection and retention of data by the Company. This is to ensure that personal data are kept within specified timelines for a periodic review and that the data is disposed of at the end of the period. All inaccurate data is rectified or deleted from the Company's database.

Personal data may be shared with the Company's affiliates for internal administrative purposes, including the processing of customer or employee's personal data.

We act as Data Processor at other times. If the Company acts as a Data Processor, the Customer becomes responsible for the implementation of effective measures and the compliance of processing activities. The following actions are taken by the Company:

- a. Designate a Data Protection Officer, when required;
- b. Maintain a written record of processing activities carried out on behalf of each Controller;
- c. Implement adequate safeguards for cross-border transfers; and
- d. Notify the Controller on becoming aware of personal data breaches, without delay.

Except expressly agreed, all personal data of a customer will either be disposed of or returned at the end of the business relationship or as stipulated under the Data Retention Schedule.

11. NOTIFICATION OF SECURITY AND DATA BREACH

There is a robust measure in place to effectively detect, report and investigate a personal data breach. A notice is sent to Management, explaining the nature of the breach. The DPO would conduct a DPIA and follow through with the incidence response plan. The DPIA process would assess and mitigate the risks to the rights and freedoms of the individuals.

Where the Company acts as a Data Processor, the Company shall without delay notify its Customers/Vendors of the personal data breaches and provide necessary information as may be required. The Data Controller/Customer retains the overall responsibility to protect the personal data and must ensure that there are appropriate safeguards in place to back up the personal data.

12. SUB PROCESSING – CROSS BORDER DATA TRANSFER

Sub-Processing: The Company ensures that its sub-processors provide the same guarantees provided on the implementation of appropriate technical and organizational measures, to meet the requirements of the processing activities.

All customers/vendors of the Company acting as Controllers, are informed in advance of the outsourced processing activities and the identity of sub-processor. Where a modification would affect the level of the protection offered by the Company, the Controller can object to the change or terminate the contract, before the data is communicated to the new sub-processor.

13. PROCESSING DATA OUTSIDE NIGERIA

The Company complies with the Regulation and is responsible to its customers/vendors to obtain their consent before transferring and processing personal data outside Nigeria, on behalf of the Customer/Vendor.

To provide adequate safeguards with applicable data protection law, the Company has in force a Contractual Standard Clauses, with all its sub-contractors/processors, who process or have access to customers' personal data. These are periodically reviewed and updated to take into cognizance changes in the Regulation.

14. POLICY REVIEW

This Policy shall be reviewed every two (2) years or as deemed necessary, in line with the applicable laws.

**Approved by the Board of Directors
On May 27, 2020**