MRS OIL NIGERIA PLC
DATA PROTECTION 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 DPP
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 Protection 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.

1.0			Plan Creation	Created the Incident Response Plan

Table of contents

1. BACKGROUND

MRS Oil Nigeria Plc. ("the Company"), is a major marketer in the downstream sector of the Nigerian Oil and Gas Industry and by the nature of its operations, the Company collects and processes certain information about individuals and corporate entities (i.e. Data Subjects) it relates with.

The purpose of the information are in respect of recruitment and employee welfare, relationship management with Regulatory Authorities, business transactions with customers, vendors, shareholders, etc. The information also includes personal data of Data Subjects, such as names of individuals, email addresses, contact telephone numbers and any other information relating to a Data Subject.

In line with the provisions of the Nigeria Data Protection Regulation, 2019 (hereinafter referred to as the "Regulation"), we are committed to our business operations and to ensure that it aligns with the local and global best practices, in the protection of the rights and privacy of our Data Subjects.

2. DEFINITIONS

a. **Consent of Data Subject** means any information freely given, specific, informed and unambiguous indication of the **data subject's** decision by which he or she, provides a statement or a clear affirmative action, and signifies agreement to the processing of personal **data** relating to him or her.
b. **Data** means character, symbols and binary on which operations are performed by a computer, which may be stored or transmitted in any form of format or device, including but not limited to electronic signals.
c. **Database** means a collection of data organized in a manner that allows access, retrieval, deletion and processing of data. It includes but not limited to structured, cached and file system type databases.
d. **Data Administrator** means a person or Organization that processes data.
e. **Data Controller** means a person who either alone, jointly with other persons or in common with other persons or as a statutory body, determines the purpose for and the manner in which personal data is processed or is to be processed.
f. **Data Portability** means the ability for data to be transferred easily from one IT System or computer to another, through a safe and secure means in a standard format.
g. **DPO** means Data Protection Officer.
h. **Data Protection Compliance Organization (DPCO)** means any entity duly licensed by NITDA to train, audit, consult and render services for the purpose of compliance with NDPR or any foreign Data Protection Law or Regulation having effect in Nigeria.
i. **Data Protection Impact Assessment (DPIA)** means the process designed to determine how data processing systems, procedures or technologies affect Data Subjects' privacy and eliminate any risks that might violate compliance.

j. **Data Subject** means a person, who can be identified directly or indirectly by an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity or a Corporation.

k. **NITDA** means Nigerian Information Technology Development Agency.

l. **NDPR** means National Data Protection Regulation.

m. **Party** means directors, shareholders, servants or privies of a contracting party.

n. **Personal Data** means any information relating to an identified or identifiable natural person (data subject);

o. **Identifiable natural person** means one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, economic, cultural or social identify of that natural person. It can be any data from a name, address, a photo, an email address, bank details, posts on social networking websites, medical information, and other unique identifier including but not limited to MAC address, IP address, IMEI number, IMSI number, SIM and others.

p. **Processing** means any operations or set of operations, which is performed on personal data or on a set of personal data, whether or not by an automated means such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or a combination, restriction, erasure or destruction.

q. **Personal Data Breach** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

r. **Record** means public record and reports in credible news media.

s. **Regulation** means the Nigeria Data Protection Regulation, 2019

t. **Sensitive Personal Data** means data relating to religious or other beliefs, sexual tendencies, health, race, ethnicity, political views, trade union membership, criminal records or any other sensitive personal information.

3. PURPOSE OF THE POLICY

The Company has the general obligation to implement technical and Organizational measures that shows that it has considered and integrated data protection into its processing activities. The purpose of this Policy is to protect the Company from the risks of a data breach, disclose how data collected are processed and stored.

4. THE GOVERNING PRINCIPLES OF DATA PROTECTION

The Company has a DPO, who amongst others ensures the compliance of the Company with the Regulations, relevant data privacy statements and data protection policy of the Company.

The Policy is in compliance with the NDPR and international best practices and seeks to protect the rights of the Company's data subjects. We have outlined below the two measures set by the Company to maintain compliance with the NDPR.

a. The measures to enforce accountability and governance.
b. The measures to demonstrate the protection of information rights of the data subject.

The Company's governing principles of data protection below is provided in Section 2.1 of the NDPR, 2019.

1. Lawful Basis for Data Processing

The Company has six (6) lawful basis for processing the data it collects:

a. Consent: The Company must obtain the consent of the Data Subject to process his/her personal data for one or more specific purposes;
b. Contract: The Data processing is required by a Data Subject who is a party to a contract for the performance of a contract to which he/she is a party in order to take steps, prior to entering into a contract;
c. Legal Obligation: The Data processing is a compliance requirement of a legal obligation to which the Company is subjected to;
d. Vital Interests: The processing of data collected is required to protect the vital interests of the Data Subject(s) or of another natural person under the Law;
e. Public Task: The Data processing is required for the performance of a task carried out in the public interest or in the exercise of official public mandate vested in the Company;
f. Legitimate Interest: The processing of Data is necessary for the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides the legitimate interest.

2. Rights of Data Subjects

Data Subjects including but not limited to employees have:

a. The right to be informed: The right to be provided with "fair processing information", typically through a Privacy Notice. The Company maintains a Privacy Notice, which is publicized on the Company's website and shall be sent upon request to anyone who requests for it.

b. The right to access: The Data Subjects have the right to access their personal data and supplementary information relating to the personal information of the

Data Subject. The right of access allows Data Subjects to be aware and verify the lawfulness of the processing. The Data Subject will have the right to obtain:

i. Confirmation that their data is being processed; ii. Access to their personal data;

iii. Other supplementary information. This largely corresponds to information that should be provided in a Privacy Notice.

c. The right to rectification: The Data Subjects have the right to rectify their personal data, if it is inaccurate or incomplete. The following additional measures will apply:

i. Where the Company has disclosed the personal data to third parties, the DPO must inform them of the rectification, if possible;
ii. The DPO must inform the Data Subjects of third parties to whom the data has been disclosed, where appropriate.
iii. The DPO will be responsible for validating whether requests for the rectification have been properly addressed.

d. The right to withdraw consent and request to delete data: The right to delete is also known as the right to be forgotten. This is to enable a Data Subject, request for the deletion or removal of personal data, where there is no compelling reason for its continued processing.

The exceptions below apply to the right of withdrawal of consent and request to delete above.

i. Data Subjects have a right to request that their personal data be deleted and to prevent processing under certain circumstances as detailed below.

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- When the Data Subject withdraws his/her consent;
- When the Data Subject objects to the processing and there is no overriding legitimate interest for continuing the processing;
- The personal data was unlawfully processed;
- The personal data has to be deleted in order to comply with a legal obligation.

ii. The Company can refuse to comply with a request for an the deletion of data, where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;

- To comply with a legal obligation for the performance of a public interest task or the exercise of official authority;
- For public health purposes in the public interest;
- Archiving purposes in the public interest, scientific research, historical research or statistical purpose; or
- The exercise or defence of legal claims.

iii. Requests for deletion of data must be submitted immediately to the DPO, who will follow the principles for right to access and right to rectification.

iv. In the event that the Company has disclosed the personal data to a third party(ies), the DPO must inform such third party(ies) of the deletion of the personal data, unless it is impossible or it involves a difficult process to do so.

e. The right to restrict processing: Data Subjects have a right to "block" or suppress the processing of personal data. When processing is restricted, the Company is permitted to store the personal data but is not permitted to further process it. The Company is required to restrict the processing of personal data in the following circumstances:

i. Where a Data Subject contests the accuracy of the personal data, the Company should restrict the processing of the data, until the accuracy of the personal data has been verified;
ii. Where a Data Subject has objected to the processing (when it was necessary for the performance of public interest, task or for the purpose of legitimate interests), and where the Company considers whether its legitimate grounds override those of the Data Subject;
iii. When Data processing is unlawful and the Data Subject opposes the deletion and requests restriction instead;
iv. If the Company no longer needs the personal data but the Data Subject requires the data to establish, exercise or defend a legal claim.

f. The right to data portability: This allows the Data Subjects to obtain and reuse personal data for their own purpose across different services. It allows them to move, copy or transfer personal data easily, from one IT environment to another, in a safe and secure way, without hindrance to usability.

This right applies:

i. To the personal data of a Data Subject provided to the Data Controllers; ii. Where the processing is based on the individual's consent or for the performance of a contract; and
iii. When processing is carried out by automated means.

5. OBTAINING CONSENT

In line with the provisions of the Regulation, the Company shall process personal data in accordance with the rights of the Data Subjects. The Company shall be guided by the following Principles when obtaining data:

i. Not to obtain the personal data except for the specific purpose for collecting the data is made to the data subject;
ii. To ensure that the consent of the data subject has been obtained without fraud, coercion or undue influence;
iii. To ensure that the data subject has consented to the processing of his or her personal data and the legal capacity to give consent. When processing, is based on consent;
iv. To request for consent in a manner which is clearly distinguishable from others, in an intelligible and easily accessible form, using clear and plain language, where the Data Subject's consent is given in the context of a written declaration;
v. To inform the Data Subjects of their rights and the ease to withdraw consent at any time;
vi. In assessing whether consent was freely given, to consider whether the performance of a contract, including the provision of a service, is conditional to obtaining consent to process personal data and if the request was not necessary or an excessive requirement to the performance of the contract;
vii. To request for consent of the Data Subject where data may be transferred to a third party for any reason.

6. DUE DILIGENCE AND PROHIBITION OF IMPROPER MOTIVES

In compliance with the Regulation, the Company shall do the following:

a. Shall not seek the consent that may endanger direct or indirect propagation of atrocities, hate, child rights violation, criminal acts, and anti-social conducts;
b. To take reasonable measures and ensure a party to any data processing contract does not have a record of violating Section 5 of the Regulation as such a party shall be accountable to NITDA or a reputable regulatory authority for data protection within or outside Nigeria;
c. The Company shall not be liable for the actions or inactions of third parties which handle the personal data of Data Subjects under this Regulation, provided that there is evidence to show that the Company informed the third parties of its obligations to Data Subjects under the Regulation, obtained an undertaking from third parties to comply with the requirements of the Regulation and performed the requisite due diligence on the third party. Third Party includes directors, shareholders, servants, customers, vendors and privies of the contracting party; and record shall include report in public record and reports in credible news media.

7. PRIVACY POLICY

The Regulation requires that the Company shall display a simple and conspicuous Privacy Policy/Notice that the class of data subjects being targeted can understand, irrespective of the medium through which such personal data were collected or processed.

The Company maintains a Privacy Policy/Notice which contains the following:

i. What constitutes the consent of a Data Subject;
ii. Description of the kind of personal data that is collected;
iii. The purpose of collecting the personal data;
iv. Technical methods used to collect and store personal information, such as cookies;
v. Access of third parties to personal data and the purpose of access;
vi. A highlight of the principles governing data processing;
vii. Available remedies in the event of violation of the Privacy Policy;
viii. The timeframe for remedy;
ix. Any limitation clause, provided that the limitation clause does not exonerate the Company from breaches of the Regulation.

8. DATA SECURITY

a. The Company understands the importance of protecting personal data from fraud or any compromise and shall protect the data against unauthorized or unlawful processing and against unlawful processing, accidental loss, destruction, damage or any form of compromise.

b. The Company hereby states that it has an IT Security Policy and supporting management systems to maintain effective and proportionate security. This includes but not limited to:

i. protecting systems from hackers;
ii. Set up firewalls and protect email systems;
iii. Store data securely with access to specific unauthorized individuals;
iv. Employ data encryption technologies;
v. Develop organizational policy for handling personal data and other sensitive or confidential data;
vi. Continuously build capacity for all employees.

9. THIRD PARTY DATA PROCESSING CONTRACTS

The Regulation requires that the Company is diligent and enters into contracts with third party(ies) in clear terms, adhering to mandatory requirements relating to contracts which are as follows:

i. Whenever the Company acts as a Data Controller, there must be a written contract in place with the Data Processor(s).
ii. When the Company acts as a Data Processor, the Company must only act on the documented instructions of the Controller (as specified in a valid written contract).
iii. On an annual basis, the DPO will review third party relationships to determine the risk posed by the processing of such data. This will be documented as part of a Data Protection Impact Assessment (DPIA).

10. OBJECTION BY THE DATA SUBJECT

The Company recognizes the right of Data Subjects to object to the processing of their data. In view of this, the Data Subject has the right to object to the processing of his/her personal data in the following instances:

a. For the purpose of scientific or historical research and statistics;
b. In relation to automated decision making and profiling;
c. For the purpose of marketing.

11. TRANSFER TO A FOREIGN COUNTRY

When transferring the personal data of a Data Subject to a foreign country or an international organization, the Company shall be subject to the supervision of the Honorable Attorney General of the Federation and the provisions of the Regulation. The following conditions must be complied with before personal data of the Company's Data Subjects are transferred to a Foreign Country:

a. The NITDA has decided that the foreign Country, or international organization has adequate level of protection;
b. The Attorney General of the Federation has considered the legal system of the foreign Country, particularly in the areas of rule of law, respect for human rights and fundamental freedom, relevant legislation. Examples are legislation on public security, defence, national security and criminal law and access of public authorities to personal data;
c. There is an implementation of such legislation, data protection rules, professional rules and security measures. This include rules which are complied with by the foreign Country or International Organization for the onward transfer of personal data to another foreign Country or international organization;

d. There is an effective implementation of one or more independent supervisory authorities in the foreign Country, or to which the International Organizations are subject to. The foreign Country or International Organization must ensure its compliance with the data protection rules, including adequate enforcement powers, for assisting and advising the Data Subjects in exercising their rights and for cooperation with the relevant authorities in Nigeria; and
e. The International commitments of the foreign Country or International Organization concerned has entered into, or other obligations arising from legally binding conventions or instruments, including participation in multilateral or regional systems regarding the protection of personal data.

12. EXCEPTIONS TO TRANSFER TO A FOREIGN COUNTRY

Where there is no decision made by NITDA or the Attorney General of the Federation on the transfer of personal data to a foreign country, the Company shall initiate the transfer or set of transfers of personal data to such a foreign country or an international organization only when:

a. The Data Subject has explicitly consented to the proposed transfer, after he/she was informed of the potential risks of such transfers to the Data Subject, as a result of the absence of an adequacy decision and appropriate safeguards and there were no alternatives;
b. The transfer is necessary for the performance of a contract between the Data Subject and the Company or the implementation of pre-contractual measures taken at the Data Subject's request;
c. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject, between the Company and another natural or legal person;
d. The transfer is necessary for important reasons of public interest;
e. The transfer is necessary for the establishment, exercise or defence of legal claims;
f. The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

In line with the provision of the Regulation, the Company shall clearly communicate warnings of specific principle(s) of data protection that are likely to be violated in the event of a transfer to a foreign country.

13. ROLES AND RESPONSIBILITIES:

The Company has identified the following key stakeholders and their responsibilities in implementing the Policy and data protection controls.

a. Board:

The Board through the Board Nomination and Corporate Governance Committee shall be responsible for ensuring governance and compliance of the Company, to the principles of the Regulation. The Board shall:

i. Ensure that the Company has and maintains a robust Data Protection Policy and complies with the principles of the Regulation;
ii. Establish strategic goals and objectives for Data Protection objectives and ensure that they are aligned with the vision of the Company;
iii. Ensure that the resources needed for the protection of data in the Company are available;
iv. Approve the Data Protection Budgets of the Company, including but not limited to training of employees.

b. The Management

The Management has its role in ensuring:

i. The importance of effective data protection and its apparent risks are properly communicated to the Company's stakeholders;
ii. The Company's stakeholders comply with the requirements of the Regulation; iii. Demonstrate leadership in areas of responsibility and avoid any penalties for non-compliance;
iv. Approval is given for data protection statements before they are circulated to the Company's stakeholders;
v. Approvals are given for responses to queries on data protection from media outlets including but not limited to newspaper agencies;
vi. Directives are provided that ensure marketing initiatives or any initiative on the use of personal data are complied with.
vii. Disciplinary procedures for data protection breaches are robust and confidential.
viii. viii. Responsible for the nomination of the members of the Executive Committee.

The members of the Executive Management Committee shall include the following:

- the Managing Director,
- the Risk and Compliance Manager,
- the Chief Internal Auditor,
- the Data Protection Officer and;
- any other nominee of the Board Nomination and Corporate Governance Committee.

c. Data Protection Officer

The Data Protection Officer shall ensure that:

i. Management is periodically updated on the data protection responsibilities, risks and issues;
ii. All Data Protection procedures and related policies are in line with the Regulation;
iii. Adequate data Protection training and advice is offered to employees who process data in the Company and other employees of the Company; iv. Data protection questions are handled and ensure everyone is covered by the Policy;
v. Requests from individuals to obtain the data of the Company are dealt with promptly;
vi. All contracts or Agreements with third parties which contain company sensitive information are properly reviewed in line with the Regulation and approved.
vii. All systems, service and equipment used for storing data meet acceptable security standards;
viii. Any third party services the Company may consider to store or process data, are evaluated.
ix. Regular checks and vulnerability scans are performed to ensure adequate security of hardware and software used in data processing.

d. Internal Audit Unit

The Chief Internal Auditor shall:

i. Provide reasonable assurance regarding the achievement of the operational objectives, such as the effectiveness and efficiency of the security controls.
ii. Ensure that the Data Protection Internal Audit systems are in place and reviewed biennially.
iii. Carry out internal audit and report findings to the Executive Management Committee;
iv. Recommend prevention and corrective action(s).
v. Report on the compliance of the Data Protection Policies to the Board Nomination and Corporate Governance Committee.

14. CONSEQUENCES

All report of breaches of any Data Protection Policy of the Company, shall be handled by the Disciplinary Committee in line with the approved Disciplinary Policy.

15. 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

This 27th day of May 2020