PRIVACY POLICY

Table of Contents

1 Introduction

1.1. This Privacy Policy (hereafter referred to as "Policy") outlines the commitment of **Mauritius Oil Refineries Ltd** (hereafter collectively referred to as "**Moroil**", "we", "us", "our") to ensure that all its processing operations involving personal data comply with the Mauritius Data Protection Act 2017 (hereafter referred to as the "**DPA**").

1.2. To seamlessly conduct our daily operations and deliver essential services associated with our business, **Moroil** is required to process personal data on a large scale. This data is sourced from various stakeholders, including its suppliers and employees. Examples of such data encompass but are not limited to, names, addresses, email addresses, identification numbers, and bank details amongst others.

1.3. **Moroil** firmly believes that every data subject has a fundamental right to exercise control over their personal data. This guiding principle is central to our commitment to data protection and privacy, and it drives our approach to safeguarding personal data with utmost respect, transparency, and accountability.

1.4. **Moroil** has put in place policies, procedures, controls, and measures to ensure maximum and continued compliance with the **DPA**, including staff training, procedure documents, and internal assessments. Ensuring and maintaining the security and confidentiality of personal and/or special categories of personal data is one of our top priorities and we are proud to operate a 'Privacy by Default and by Design' approach, assessing changes and their impact from the start and designing systems and processes to protect personal data at the core of our business purpose.

2. Purpose

2.1. The purpose of this Policy is to ensure that **Moroil** meets its legal, statutory, and regulatory requirements under the **DPA**, to ensure that all personal and special categories of personal data are processed compliantly and in the data subjects' best interests.

2.2. The **DPA** includes provisions that promote accountability and governance and as such **Moroil** has put comprehensive and effective governance measures into place to meet these provisions. Such measures aim to ultimately minimise the risk of breaches and uphold the protection of personal data.

2.3. This Policy also serves as a reference document for employees and directors on the responsibilities of handling and accessing personal data and data subject requests.

3. Scope

3.1. This Policy applies to the processing of personal data for any data subject, regardless of format, structure, or media, in both electronic and hardcopy formats. The entire information lifecycle is considered under this policy, including collection, storage, processing, disclosure, transmission, retention, archiving, disposal, and deletion of personal data.

4. Objectives

4.1. **Moroil** ensures the safe, secure, ethical, and transparent processing of all personal data and has stringent measures to enable data subjects to exercise their data protection rights. **Moroil** has developed the below objectives to meet data protection obligations and to ensure continued compliance with **DPA**.

Moroil ensures: -

- the protection of the rights of individuals with regard to the processing of personal data;
- the implementation and maintenance of a privacy policy, procedure, and training program for compliance with the **DPA** and its principles;
- every business practice, function and process carried out by **Moroil**, is monitored for compliance with the **DPA** and its principles;
- data is only processed where we have met the lawfulness of processing requirements;

- that the processing of special categories of data is in accordance with the **DPA**;
- that consent is recorded at the time it is obtained and evidence such consent to the Data Protection Commissioner where requested;
- that it has robust and documented complaint handling and data breach controls for identifying, investigating, reviewing, and reporting any breaches or complaints with regard to data protection;
- clear lines of reporting and supervision with regards to data protection;
- that it stores and destroys all personal data, in accordance with the **DPA** timeframes and requirements;
- that any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible, and easily accessible form, using clear and plain language;
- employees are aware of their rights under the **DPA** and are provided with an Employee Privacy Notice;
- where applicable, a record of processing operations is maintained in accordance with Section 33 of the **DPA**; and
- appropriate technical and organisational measures and controls for personal data security are developed and documented.

5. Consequences of Non-Compliance

5.1. Compliance with the **DPA** is of utmost importance to **Moroil**. **Moroil** understands that failure to adhere to the provisions stipulated in the Act may lead to penalties as outlined in the legislation. It is thus **Moroil**'s responsibility to take necessary actions to prevent such penalties including continuous training of its staff, rigorous monitoring of its data processing activities, and proactive measures to address any potential risks.

5.2. Wilful and deliberate non-compliance with this Policy can expose **Moroil** to significant potential regulatory sanctions, fines and criminal liability.

5.3. Employees who fail to comply with this Policy may be subject to disciplinary action which may include dismissal and could, in some instances, be exposed to personal liability such as fines and/or imprisonment under the applicable laws.

5.4. Non-compliance with this Policy by suppliers, service providers and contractors can result in the termination of any ongoing contractual relationships between the suppliers, service providers and contractors and **Moroil**.

6. Definitions

Definition	Interpretation
Biometric data	means any personal data relating to the physical, physiological, or behavioral characteristics of an individual which allows his unique identification, including facial images or dactyloscopic data.
Commissioner	means the Data Protection Commissioner.
Consent	means any freely given specific, informed, and unambiguous indication of the wishes of a data subject, either by a statement or a clear affirmative action, by which he signifies his agreement to personal data relating to him being processed.
Controller	means a person who or public body which, alone or jointly with others, determines the purposes and means of the processing of personal data and has decision making power with respect to the processing.
Data Subject	means an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual.
Data Protection Officer (hereafter	means an independent person responsible for ensuring that a **Moroil** complies with the **DPA**.

referred to as the '**DPO**')	
Encryption	Encryption is a mathematical function using a secret value—the key—which encodes data so that only users with access to that key can read the information.
Genetic data	means personal data relating to the general characteristics of an individual which are inherited or acquired, and which provide unique information about the physiology or health of the individual and which result, in particular, from an analysis of a biological sample from the individual in question.
Physical or mental health	in relation to personal data, includes information on the provision of health care services to the individual, which reveals his health status.
Personal data breach	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
Processor	means a person who, or public body which, processes personal data on behalf of a controller.
Processing	means an operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
Profiling	means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.
Pseudonymisation	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the

	use of additional information and the additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual.
Special categories of Personal Data	in relation to a data subject, means personal data pertaining to – (a) his racial or ethnic origin; (b) his political opinion or adherence; (c) his religious or philosophical beliefs; (d) his membership of a trade union; (e) his physical or mental health or condition; (f) his sexual orientation, practices or preferences; (g) his genetic data or biometric data uniquely identifying him; (h) the commission or alleged commission of an offence by him; (i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings; or (j) such other personal data as the Commissioner may determine to be sensitive personal data.
Third party	means a person or public body other than a data subject, a controller, a processor, or a person who, under the direct authority of a controller or processor, who or which is authorised to process personal data.

7. Principles Relating to Processing of Personal Data

7.1. Section 21 of the **DPA** outlines six privacy principles. These principles serve as fundamental conditions that controllers must adhere to while processing personal data. The principles are:

7.1.1. <u>Lawfulness, fairness, and transparency</u>

- Before processing personal data, **Moroil** will always establish a valid legal basis as outlined in the **DPA**. All departments and sections will document and maintain the lawful basis for processing personal information across all processes and operations. The legal bases are detailed in Section 12 of this policy.

- When relying on consent as a legal basis, **Moroil** will ensure that the consent has been obtained freely, explicitly, and unambiguously from the data subjects and that the data subjects can revoke the consent at any time.

- **Moroil** will strive to treat individuals' personal data with fairness and respect. This entails providing information to data subjects about how **Moroil** processes their personal data through clear and concise privacy notices.

7.1.2. Purpose limitation

- **Moroil** will, at all times, use personal data solely for specific purposes defined and a record of these purposes must be documented and maintained by the business department and section making use of the personal information.

- Data subjects will be made aware of the purposes for which **Moroil** collects and uses their personal data at the point where it is collected or during any future interactions with the data subject.

- Data processing activities will be regularly reviewed to ensure they remain aligned with the purposes for which the personal data was collected.

- Any additional processing of personal information across the **Moroil** ecosystem must be compatible with the original purpose(s) for which it was collected.

- For any incompatible or additional purpose of processing, data subjects will be informed of the new purpose and, where applicable, requested for their consent for such further processing.

7.1.3. Data minimisation

- **Moroil** will collect and process only the minimum amount of personal data necessary to achieve the specified purposes.

- **Moroil** will minimise data shared with third parties to align with minimum business requirements; this will be considered on a case-by-case basis.

7.1.4. Accuracy

- **Moroil** will take reasonable steps to ensure that all personal data and information is kept accurate, complete, up to date, and not misleading as is necessary for the purposes for which it is processed.

- Adequate data quality guidelines and processes will be devised to ensure that personal data held by **Moroil** is kept up-to-date, accurate, and complete and that the integrity of the personal data is maintained during processing.

- This principle is also linked to the right of rectification which confers upon data subjects the right to correct inaccurate personal data. **Moroil** will devise appropriate procedures to ensure such rights are upheld.

7.1.5. Storage limitation

- **Moroil** recognises the importance of limiting the retention of personal data to what is necessary for the purpose for which the personal data is processed. Appropriate retention schedules will be developed and maintained, considering legal, regulatory and business requirements as well as the requirement not to retain personal data for longer than is necessary.

- **Moroil** will also ensure that appropriate mechanisms for the disposal of personal data are put in place and that such procedures are documented. Disposal techniques will need to be carefully chosen based on several factors such as:
    - The nature and extent of the personal data to be disposed of,
    - Whether or not there is metadata associated with the personal data, or
    - The physical characteristics of the media on which the personal data is stored.

- Please refer to our **Record Management Procedure** for more information on personal data retention and disposal.

7.1.6. Data Subjects' Rights

- **Moroil** commits to respect the rights of data subjects as provided by the **DPA** and per international best practices, including the right of access, the right to rectify, erase, restrict and object to the processing of personal data, the right to object to the processing of their personal data for direct marketing and the right to withdraw consent.

- **Moroil** will devise procedures to ensure that data subjects are provided with appropriate information about the processing of their personal data and to meet other applicable obligations to data subjects related to the processing of their personal data.

- In addition, **Moroil** will also design public-facing privacy notices to inform relevant data subjects about how **Moroil** processes their personal data.

- Please refer to our **Data Subject Rights Request Procedure** for more information on the rights of the data subjects and how to handle any requests from data subjects.

8. Accountability

8.1. **Moroil** recognises the significance of accountability in ensuring the lawful and transparent processing of personal data. This commitment aligns with the principles outlined in Section 22 of the **DPA**. Adequate and appropriate technical and organisational measures will be established to ensure that the processing of personal data is compliant with the **DPA** such as:

- adopting and implementing data protection policies, procedures and guidelines (where proportionate);

- putting written contracts in place with organisations that process personal data on **Moroil**'s behalf;

- keeping a record of all processing operations;

- implementing appropriate security measures to protect personal data;
- performing a data protection impact assessment for high-risk processing operations;
- complying with the requirements for prior authorisations from or consultations with the Commissioner;
- designating an officer responsible for data protection compliance issues;
- recording and reporting personal data breaches.

8.2. Further, **Moroil** will implement policies and mechanisms for ongoing verification of the effectiveness of these measures through regular assessments, audits, and reviews.

9. Registration/Renewal of Registration with the Data Protection Office

9.1. Under section 14 of the **DPA**, every controller and processor needs to register with the Data Protection Commissioner.

9.2. The validity of the registration certificate is 3 years. 3 months before its expiration, **Moroil** will need to renew the registration certificate per section 18 of the **DPA**.

9.3. The Mauritius Oil Refineries Ltd is registered with the Data Protection Office as a Controller and Processor of personal data. The Registration Number is C5178.

10. Role of the Data Protection Officer (hereafter referred to as the "DPO")

10.1. Section 22(2)(e) of the **DPA** requires that every Controller of personal data in Mauritius must appoint a **DPO** who will be responsible for data protection compliance issues.

10.2. The **DPO** is required to work within an independent environment and manner, report to the highest management level and have adequate resources to enable the controller to meet its obligations under the **DPA**.

10.3. The **DPO** will be responsible to:

- Inform and advise the controller and its employees about their obligations to comply with the **DPA** and other data protection laws.

- Monitor compliance with the **DPA** and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments, train staff, and conduct internal audits.

- Be the first point of contact for the Data Protection Office and for individuals whose data are processed (employees, customers, amongst others).

10.4. Any questions on the **DPA** should be addressed to the **DPO**. Contact details of the **DPO** of **Moroil** is as follows:

- Email Address: dpo@moroil.mu
- Phone number: 206 9800
- Address: Quay Road, Port Louis.

11 Record of Processing Operations (hereafter referred to as "RPO")

11.1. Section 33 of the **DPA** provides that "every controller or processor shall maintain a record of all processing operations under his or its responsibility". **Moroil** will thus determine and securely maintain a comprehensive Record of Processing Operations in support of its obligations for processing personal data, for overseeing and ensuring compliance with the **DPA**.

11.2. Relevant departments and sections will assist the **DPO** in maintaining the RPO with the necessary information about their data processing activities. This information will form the basis of a data inventory, crucial for overseeing and ensuring compliance with the **DPA**.

11.3. To maintain an accurate and up to date RPO, all departments and sections within the **Moroil** will also be responsible for informing the **DPO** of any changes to the personal data they collect and process.

12 Legal Basis for Processing Personal Data

12.1. **Moroil** needs to identify legal bases for its data processing activities. These legal bases will be documented in the Record of Processing Operations and on request, make the record available to the Data Protection Office. The lawful bases which **Moroil** will rely on for processing personal data are where:

- The data subject has given consent to the processing of their personal data for one or more specific purposes;
- The processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;
- The processing is necessary for compliance with a legal obligation to which **Moroil** is subject to;
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- The processing is necessary for the performance of any task carried out by a public authority; or
- The processing is necessary for a purpose that concerns a legitimate interest of **Moroil**, or of a third party to whom the personal data is provided, except where such interest is overridden by the interest to protect the fundamental rights and freedoms of the data subject, and particularly the right to privacy.

13 Processing Special Categories of Personal Data

13.1. **Moroil** recognises that certain categories of personal data are classified as sensitive personal data and that the processing will be strictly conducted in accordance with the **DPA**. **Moroil** will ensure that there is a lawful basis for processing sensitive personal data namely where:

- The data subject has given explicit consent to the processing of the personal data;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject;
- Processing relates to personal data which are manifestly made public by the data subject;
- Processing is necessary for the establishment, exercise, or defence of legal claims or whenever courts are acting in their judicial capacity.
- Processing is necessary for the assessment of the working capacity of an employee or medical diagnosis.

14 Security of Processing

14.1. In accordance with Section 31 of the **DPA**, **Moroil**, as a controller is committed to upholding the highest standards of security in the processing of personal data. At the time of determination of processing means and during the actual processing, we undertake to implement appropriate security and organisational measures to:

- prevent unauthorised access to personal data under our control;
- maintain the integrity of the data, preventing any unauthorised alterations or tampering during processing;
- restrict and control the disclosure of personal data thereby maintaining the confidentiality of the data;
- mitigate the risk of accidental loss. This includes secure storage, regular backups, and disaster recovery planning;
- prevent unauthorised destruction of personal data ensuring its retention in accordance with applicable legal and regulatory requirements.

15 Privacy by Design and by Default

15.1. **Moroil** is committed to ensuring that data protection considerations are at the forefront of its operations. Its approach entails embedding data protection measures into the very architecture of its systems and processes from their inception to their execution.

15.2. In addition, **Moroil** will ensure that the default settings of its systems prioritise the protection of personal data, limiting the amount of data to what is strictly necessary for the intended purpose.

15.3. Checklists will be designed for use by relevant departments to assess the implementation of Privacy by Design and by Default.

16 Data Protection Impact Assessment (DPIA)

16.1. In compliance with Section 34 of the **DPA**, **Moroil** recognises the importance of conducting Data Protection Impact Assessments (DPIAs) where processing operations may pose a high risk to the rights and freedoms of data subjects due to their nature, scope, context, and purposes.

16.2. **Moroil** will take into consideration the guidelines issued by the Data Protection Office on criteria for assessing high-risk processing operations when assessing the need for a DPIA.

16.3. Whenever a DPIA will need to be conducted, the relevant department will need to consult with the **DPO** for assistance in this process.

17 Breach Management

17.1. **Moroil** understands its obligations where it is acting as a data controller to notify the Commissioner of a personal data breach where feasible, within 72 hours after becoming aware of it. Should there be any delay in notification, **Moroil** will provide the Commissioner with the reasons for the delay, as mandated by the **DPA**.

17.2. Moreover, if a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, **Moroil** will, after notifying the Commissioner, promptly communicate the breach to the affected data subjects.

17.3. To facilitate a swift and effective response, employees are required to promptly report any personal data breaches to both the **DPO** and their respective head of department as soon as they become aware of the breach.

17.4. Please refer to our Data Breach Response Plan for more information on handling data breaches.

18 Third-Party Processor/Vendor Management

18.1. **Moroil** may utilise external processors for certain processing activities and hence will need to establish a set of rules and procedures to follow which will govern business relationships with third-party service providers, namely with regard to identifying and assessing vendors as well as evaluating their privacy risk.

18.2. Vendor Assessment will be done in accordance with the Processor Selection Policy and will include risk assessments and further due diligence requirements dependent on the services that they will provide to **Moroil**, the types, sensitivity, and volumes of personal information to be processed by the third party (if any), and the risk and potential impact posed to any data subjects by such processing.

18.3. Standard contractual agreements for all third parties will include privacy, data protection, information security and data handling clauses.

18.4. Please refer to our **Processor Selection Policy** for more information on how to conduct Vendor Management.

19 Disclosure of Personal Data

19.1. **Moroil** may disclose personal data to third parties or other stakeholders (for instance, insurance companies and regulatory authorities) during its processing operations. **Moroil** will consider the following when disclosing personal data:

- Records of personal data shared/ transferred to or from third parties involved in the process will be kept.
- While disclosing/ sharing personal data with third parties, the data minimisation rule will be applied to the records so that only required information is shared with third parties.
- Informing the data subjects of any disclosure through the privacy notices.
- Whether the disclosure is authorised by any written law or required by courts, tribunal, and administrative authorities.

19.2. It is important to note that certain exchanges of information between Ministries, Government departments, and public sector agencies, which are required on a need-to-know basis, fall outside the scope of the **DPA**.

20 Transfer of Personal Data outside of Mauritius

20.1. **Moroil** understands the importance of the secure and lawful transfer of personal data whether it involves cross-border transfers to other organisations, including the storage of personal data on the Cloud. **Moroil** is aware that these actions necessitate meticulous considerations and strict adherence to the provisions outlined in Section 36 of the **DPA**. To ensure the lawful and secure international transfer of personal data, the following steps will be followed:

- Identify and document the reasons for personal data transfer.
- Identify the destination country or countries.
- Identify if **Moroil** can rely on any lawful basis for the transfer as stipulated under section 36 of the **DPA** such as providing proof of appropriate safeguards to the Commissioner, consent provided by the data subject, transfer necessary for performance of a contract

between the data subject and **Moroil** or the implementation of pre-contractual measures or conclusion or performance of a contract concluded in the interest of the data subjects between **Moroil** and another person amongst others.

- Establish appropriate safeguards such as:
  - Agreements such as Standard Contract Clauses or Cross Border Agreements.
  - Security measures such as encryption and secure channels must be implemented to protect any transfer.

21 Training

21.1. **Moroil** aims to raise awareness, build a strong data protection culture, and foster a sense of responsibility among its employees. Through ongoing training and education that will be planned, the employees will be better equipped to handle personal data responsibly, mitigating data protection risks and ensuring compliance with the **DPA**.

22 Penalties

22.1. **Moroil** acknowledges its obligations and responsibilities under the **DPA** and comprehends the severity of any breaches under the law.

22.2. We recognise that under the **DPA**, in case of a violation of the Act occurs without specific penalties outlined, individuals found guilty may face a fine not exceeding MUR 200,000 and imprisonment for a term not exceeding 5 years.

23 Policy Update

23.1. **Moroil** may update this policy from time to time to reflect best practices in data protection, security, and control and to ensure compliance with any changes or amendments made to the **DPA**.

24 Related Documents

24.1. The Policy must be read in conjunction with the following:

- Business Continuity Management Policy
- Information Security Policy
- Record Management Procedure
- Data Subject Rights Request Procedure
- Data Breach Response Plan
- CCTV Policy
- Privacy Notices
- Processor Selection Policy
- Cookie Notice

Name: Akhtar Dawood Date: 14 February 2025

Signature: DocuSigned by: Akhtar Dawood E367A11AAE90492...