DATA SUBJECT RIGHTS REQUEST PROCEDURE

Table of Contents

1. Introduction…… 3

2. Purpose…… 3

3. Scope……. 3

4. Roles, Responsibilities and Accountabilities.....4

5. Data Subject Rights 4

6. Procedure For Handling Data Subject Access Requests (“DSAR”) 5

7. Handling other requests 11

8. Timeframe…… 14

9. Record Management.....14

10. Complaints.....15

11. Compliance, Monitoring and Review.....16

12. Glossary of Abbreviations and Definitions 16

13. Appendix A: Data Subject Rights Request Form.....16

1. Introduction

1.1. At **Mauritius Oil Refineries Ltd** (hereafter "**Moroil**", "we", "us", or "our"), we recognise that every data subject has a fundamental right to exercise control over their personal data. **Moroil** is committed to respecting those rights in compliance with the Mauritius Data Protection Act 2017 (hereafter referred to as the "**DPA**").

1.2. **Moroil** commits to providing clear and understandable information to data subjects about how to exercise their rights and further commits to respond to data subjects within a reasonable timeframe as defined in this Data Subjects Rights Request Procedure ("Procedure").

2. Purpose

2.1. The objectives of this Procedure are to:

2.1.1. Define and set out the steps for handling of data subject rights requests within **Moroil**.

2.1.2. Ensure transparency and provide clarity regarding data subject rights for individuals and stakeholders, while also ensuring that **Moroil** maintains clear and well-defined processes for the management and resolution of data subject rights requests.

2.1.3. Familiarise and educate **Moroil's** employees about their respective roles and responsibilities in safeguarding the privacy and rights of individuals when handling personal data, as well as to promote a culture of data protection compliance.

3. Scope

3.1. This Procedure shall apply to:

3.1.1. all employees and departments of **Moroil** who handle and process personal data, where **Moroil** is acting as a Controller.

3.1.2. all third parties (service providers) involved in the processing of personal data on behalf of **Moroil**.

4. Roles, Responsibilities and Accountabilities

Members	Roles, Duties & Responsibilities
Data Protection Officer (hereafter referred to as the '**DPO**')	• Responsible for overseeing the implementation of this Procedure and ensuring compliance with the **DPA**. • Provide guidance and training to staff and relevant departments on handling data subject rights requests. • Review and assess the validity of data subject rights requests where required. • Ensure that responses to data subject rights requests are provided within the specified timeframe. • Maintain records of all data subject rights requests and their outcomes in a log, which is the Data Subject Rights Request Log. • Be the primary point of contact for data subjects submitting data subject rights requests. • Acknowledge the receipt of the request and initiate the identity verification process.
Departments at **Moroil**	• Collaborate with the **DPO** to verify the identity of the data subject and validate the request's authenticity. • Adhere to the steps outlined in this document for responding to data subject rights requests.
All Employees	• All employees and personnel involved in the processing of personal data will be responsible for promptly notifying the **DPO** of any data subject rights requests received from data subjects.

5. Data Subject Rights

5.1. The rights of the data subjects are as follows:

5.1.1. **Right to be informed**: Data subjects have the right to be informed of any personal data that **Moroil** holds on them and how **Moroil** is processing their data.

5.1.2. **Right of Access:** Data Subjects have the right to request access to the personal data **Moroil** hold about them. This includes the right to obtain confirmation of whether we process your personal data and to receive a copy of that information.

5.1.3. **Right to Rectification:** If a data subject believes that the personal data **Moroil** hold about him/her is inaccurate or incomplete, he/she has the right to request that we correct or update it.

5.1.4. **Right to Erasure:** In certain circumstances, data subjects may have the right to request the erasure of their personal data. This includes situations where their personal data is no longer necessary for the purposes for which it was collected, or they withdraw their consent and there is no other legal basis for processing.

5.1.5. **Right to Restriction of Processing:** Data Subjects have the right to request the restriction of processing of their personal data under certain conditions. This means **Moroil** will need to temporarily suspend the processing of their personal data, such as when the data subjects contest the accuracy or when they object to the processing.

5.1.6. **Right to Object:** Data Subjects have the right to object to the processing of their personal data for certain reasons, such as direct marketing or legitimate interests. If they exercise this right, **Moroil** will no longer process their personal data unless we can demonstrate compelling legitimate grounds that override your interests, rights, and freedoms.

5.1.7. **Right to Withdraw Consent:** If **Moroil** relies on consent as the legal basis for processing personal data, data subjects will have the right to withdraw consent at any time. This will not affect the lawfulness of processing based on consent before its withdrawal.

6. Procedure For Handling Data Subject Access Requests ("DSAR")

6.1. How should DSARs be processed by Moroil after receipt?

6.1.1. Report to the Data Protection Officer (hereafter referred to as the '**DPO**')

a) When a DSAR is received by any employee of **Moroil**, other than the **DPO**, the request should immediately be reported to the **DPO**.

b) The **DPO** will then channel the request to the concerned Department for assistance, where required, in processing the request received.

c) The **DPO** will register the request in the Data Subject Rights Request Log.

6.1.2. Validity Check

6.1.2.1. The **DPO** will need to consider the following before deciding how to respond to the request:

a) Request may be made in writing or verbally. (A Data Subject Rights Request Form, provided in Appendix A, can be used. However, it is not mandatory that the request is done only through this form).

b) Requests should include the contact details of the person seeking access to their information.

c) A request sent by email, fax or on the website is as valid as one sent in a hard copy form.

6.1.2.2. The **DPO** must make an initial assessment of the request to determine whether the request is manifestly unfounded or excessive, and whether **Moroil** will respond to such request.

6.1.2.3. Whether a request is manifestly unfounded or unreasonable, is to be determined on a case-to-case basis.

6.1.2.4. Examples of instances where a request can be found unfounded or unreasonable are as follows:

a) The same person systematically or frequently sends different requests to **Moroil** in a short lapse of time;

b) If the requestor is not a data subject of **Moroil**;

c) If the information being requested is not held by **Moroil** and was not provided to **Moroil** at all.

6.1.3. Identity verification

6.1.3.1. Before processing a request, the requestor's identity must be verified to avoid personal data of one individual being sent to another, either accidentally or as a result of deception.

6.1.3.2. Information requested for identity verification will be considered on a case-to-case basis, in accordance with a risk-based approach. The more sensitive the data, the more information will be asked to authenticate the DSAR.

6.1.3.3. **Moroil** will not ask for additional information if the identity of the requestor is obvious, for example if the request is made by a current employee whom the **DPO** and/or the concerned Head of Department knows personally.

6.1.3.4. Examples of identity verification measures are:

a) Conducting sufficient internal checks to validate the request, based on information **Moroil** already knows about the individual;

b) Cross-checking whether the signature on the Data Subject Request Form is the same as on other available forms or agreements signed by the data subject, for instance on contracts, or contracts of employment;

c) Verifying whether the Data Subject Rights Request form has been made when the data subject was already in an authenticated state, i.e., employees of **Moroil** sending request from their corporate/work email account.

d) Contacting the concerned data subject and asking additional questions to verify their identity, such as asking for a piece of information held in the data subject's records that we would expect the data subject to know.

6.1.4. Verifying if the DSAR was made by a third party or representative

6.1.4.1. Anyone with full mental capacity can authorise a representative/third party to help them make a DSAR.

6.1.4.2. Before disclosing any information, the **DPO** must be satisfied that the third party has the authority to make the request on behalf of the requestor and that the appropriate authorisation to act on their behalf is included in the request form.

6.1.5. Verifying completeness of the request

6.1.5.1. If the request is deemed to be incomplete, the **DPO** will send the individual a Data Subject Rights Request Form with a covering letter within two working days as from the date of receipt of the request to communicate same. If after three months no reply has been received, the request will be destroyed in a confidential and secure manner.

6.1.6. Acknowledging a request

6.1.6.1. Where a DSAR is deemed valid and the identity of the data subject has been confirmed, the **DPO** will then send to the data subject an acknowledgement letter or email within two working days and will make a request to the concerned Department for assistance in information gathering.

6.1.6.2. If **Moroil** decides to decline the request, or the request is assessed as manifestly unfounded or unreasonable, a written explanation to the data subject will be provided by the **DPO** within two working days as from the date of receipt of the request to communicate the same and the data subject will be informed of his/ her right to challenge this decision and complain to the Data Protection Office.

6.2. Information Gathering

6.2.1. Within eight additional working days from the date on which the **DPO** transferred the request to the concerned Department, the latter, with the assistance of the IT Department, where applicable, will gather any manually or electronically held information.

6.2.2. The concerned Department will process the DSAR in accordance with what the requestor has asked for, specifically when the request is for information within a certain time period.

6.2.3. When collating the information, the concerned Department will ensure that any information that is being requested has not been missed and will look at both current and archived information.

6.2.4. Manual and Electronic Data

6.2.4.1. For staff data, the information is located in:

- physical files
- **Moroil's** local server

6.2.4.2. Any other information related to customers, suppliers and so forth will be located on information systems such as on SAP Business One, Sicorax and OneDrive server.

6.2.4.3. Information contained in paper files will be in filing cabinets held by concerned departments.

6.2.5. Incomplete or inaccurate information available

6.2.5.1. If the personal data on file or electronic systems is found to be inaccurate, the personal data will not be amended and sent out. The data will be provided in its current state to the requestor. A note may be provided to the requestor apologising for the error in the data, stating that the information was inaccurate but will now be amended. A revised copy will then need to be provided.

6.2.5.2. Similarly, if personal data that should have been previously deleted/ disposed of, i.e., the data has been retained for longer than is appropriate, then it will not be destroyed. A copy of the data will be provided to the requestor with a statement that the data should not have been retained. Upon data deletion, the requestor will further be advised that the data has now been removed from the file and safely destroyed.

6.2.5.3. Data protection laws require organisations to retain accurate and up-to-date records. If it is noted that if information is repeatedly inaccurate or is not being disposed of promptly, this will be raised with the **DPO** as a risk, and it will be ensured that the issue is appropriately addressed.

6.2.6. Data changed due to a routine update before disclosure

6.2.6.1. A routine update of the data may result in personal data being amended or even deleted while the **DPO** is dealing with the request (for example, change in address, update in contact details).

6.2.6.2. The amended/modified information will be sent to the data subject even if the information is different from the information **Moroil** held when the request was first received.

6.2.7. Data has already been deleted or anonymised

6.2.7.1. If the requested information has already been deleted according to its set retention period (as provided in the Retention and Disposal Schedule of the Records Management Procedure), the following steps should be taken:

a) **Confirm Deletion**: The **DPO** will ensure that the data has indeed been deleted as per its set retention period.

b) **Justification**: The **DPO** will provide a clear explanation to the data subject, stating the legal basis or legitimate reasons for the data's deletion and citing the relevant sections from the Records Management Procedure, where required.

c) **Restoration (If Possible)**: If the **DPO** is no longer able to identify the personal data as a result of a de-identification process, he/she will not seek to re-identify

the data to provide a copy to the data subject. However, where there is a legitimate request or where required by law, the **DPO** may request additional information from the data subject to enable re-identification and subsequent disclosure where feasible.

6.2.7.2. If the deletion of the data was a mistake or unauthorised, and the data subject's data can be restored, the **DPO** with the help of the IT Department will proceed with the restoration of the data and inform the data subject accordingly.

6.3. Disclosure of third party information

6.3.1. In some cases, responding to a DSAR may mean disclosing information relating to another third-party individual. The **DPO** will first consider options such as summarising the information, deleting names or other identifiers, and data masking rather than providing documents/ files which may contain third-party information. However, if it is impossible to separate the third-party information, the **DPO** will only disclose such third-party information if:

a) the third party has consented to the disclosure; or
b) it is reasonable to comply with the request without the third-party's consent.

6.3.2. In determining whether it is reasonable to proceed with the DSAR without the third party's consent, the **DPO** will apply the balancing test by weighing the data subject's rights against the third party's rights with respect to their data. In applying the balancing test, the following circumstances will be considered:

a) the type of information to be disclosed;
b) any duty of confidentiality owed to the third-party individual;
c) any steps **Moroil** has taken to try to get the third party's consent;
d) any stated refusal of consent by the third party;
e) whether or not the third-party information is already known by the data subject, or is generally available to the public; and
f) the significance of the information to the requestor.

For access to CCTV images and footage by third parties, please refer to our CCTV Policy for more information.

6.4. **Information provision**

6.4.1. Once the concerned Department has collated the personal data held on the data subject, either the **DPO** or the concerned Department will communicate the requested information to the data subject as follows:

a) provide the information by compiling a report with the information obtained from information systems and paper based files; or

b) providing a copy of the information.

6.4.2. The information will be concise, transparent, intelligible and where applicable, in a structure, commonly used, machine-readable format, using clear and plain language. Internal Codes or Identification numbers used at **Moroil** will be translated before being disclosed. This will be done as soon as possible and within the timeframes set out in Section 8.

6.4.3. Where the data subject has requested the data to be transferred to another organisation, the concerned Department or the **DPO** will provide the information in a machine-readable format or where applicable in the format requested.

6.4.4. The **DPO** should the update the Data Subject Rights Request Log accordingly.

6.4.5. After the response has been sent to the requestor, the DSAR will be considered closed and archived by the **DPO**.

7. Handling other requests

NOTE 1: The procedure to address other data subject rights requests such as a request for rectification, a request to object to a certain processing activity or a request to delete information is similar as described above. Further steps to respond to these requests have been elaborated under Sections 7.1 and 7.2 respectively.

NOTE 2: For the right to withdraw consent, please refer to the procedure detailed under Section 7.3 respectively.

7.1. Right to Rectification

7.1.1. Within two additional working days from the date on which the **DPO** transferred the request to the concerned Department, the latter will process the request to locate and verify whether the personal data in question is incorrect or not.

7.1.2. Should the personal data in **Moroil's** records be incorrect, then the concerned Department will amend the details immediately as directed by the data subject and keep a record of the change(s) and reason(s).

7.1.3. The **DPO** will then inform the data subject in writing, within two additional working days of the correction and where applicable, provide the contact details of any third-party to whom the personal data has been disclosed and the steps taken to inform the third-party recipients of the rectification to be made pertaining to the shared personal data (Please refer to Section 6.4).

7.1.4. If for any reason, **Moroil** is unable to act in response to a request for rectification, a written explanation to the data subject will be provided by the **DPO** within two working days as from the date of receipt of the request to communicate same and the data subject will be informed of his/ her right to complain to the Data Protection Office.

7.1.5. The **DPO** will then close the request and update the Data Subjects Rights Request Log accordingly.

7.2. Right to Erasure, Right to Restriction and Right to Objection

7.2.1. When processing a request for the erasure of personal data, the Record Owner's Responsibility Undertaking will need to be checked by the **DPO** to see if there is a disposal hold on the personal data. In the affirmative, the **DPO** will add the same in the Data Subject Rights Request Log accordingly.

7.2.2. If the request is to erase the personal data, the concerned Department, with the assistance of IT Department where applicable, will delete the personal data from all the records of **Moroil** including back-ups and archives in the established timeframe as provided under Section 8.

7.2.3. If the request received is to restrict or object to the processing of personal data, the concerned Department, with the assistance of the IT Department where applicable, will restrict or stop the processing of the personal data in the established timeframe as provided in Section 8, for example by preventing users from accessing the data or transferring the data subject in 'do-not-contact' lists.

7.2.4. The **DPO** will then inform the data subject in writing of the erasure, restriction or objection as applicable.

7.2.5. If for any reason, the **DPO** is unable to act in response to a request for erasure, restriction or objection, a written explanation to the data subject will be provided by the **DPO** within two working days as from the date of receipt of the request to communicate same and the data subject will be informed of his/ her right to challenge this decision and complain to the Data Protection Office.

7.2.6. The **DPO** will then update the Data Subject Rights Request Log accordingly.

7.3. Withdrawal of Consent

7.3.1. The data subject has the right to withdraw his/ her consent at any time, for legitimate, reasonable grounds compelling him/ her at that particular time.

7.3.2. The concerned Head of Department, with the assistance of the **DPO**, will ensure that the method provided to the data subject to withdraw consent is consistent with the mechanism used for obtaining consent where possible. For example, where the consent has been collected via email, the data subject will not be asked to exercise his/ her right to withdraw consent by fax, but rather via email itself.

7.3.3. The withdrawal request will be documented by the **DPO** and the **DPO** will also consider updating the Data Subject Rights Request Log.

7.3.4. In cases where the withdrawal of consent necessitates the erasure of personal data, the **DPO**, in collaboration with the concerned Head of Department, will undertake an assessment to determine whether such data deletion would impose a disproportionate effort. The concerned Head of Department and the **DPO** will also record this in the Consent Log and the Data Subject Rights Request Log respectively.

7.3.5. Each withdrawal request will be meticulously evaluated on a case-by-case basis to ensure compliance with **DPA**.

7.4. Informing Third Parties with whom personal data was shared of the request obtained

7.4.1. When **Moroil** receives requests from data subjects for withdrawal of consent, or objections about their personal data, the **DPO** will need to inform any third parties (processors, service providers or other entities amongst others) with whom the personal data has been shared of such requests, by providing them with all the relevant details pertaining to the requests.

7.4.2. The third parties will also be informed of the effective date of the withdrawals of consent or objections.

7.4.3. The **DPO** will request an acknowledgement from the third parties upon receipt of the notification and communicate with the third parties to oversee that the necessary actions are taken in response to the data subject's request and seek confirmation that they have attended to the request.

8. Timeframe

8.1. Acknowledging requests will be done **within two (2) working days**.

8.2. The DSAR will be responded to within one month and can be extended by a further month in the case of complex requests. Upon receipt of the request, the Department concerned must within **fifteen (15)** working days:

8.2.1. Identify the requisite data;

8.2.2. Complete the requested action(s);

8.2.3. Provide an update to the **DPO**.

8.3. Right to rectification and objection will be responded to without undue delay and **within five (5) working days**. However, it can be extended **fifteen (15) working days** in the case of complex requests.

8.4. Right to erasure will be responded to **within fifteen (15) working days** and can be extended by another **fifteen (15) working days** in the case of complex requests.

8.5. After the response has been sent to the requestor, the request will be considered closed and archived by the **DPO**.

9. Record Management

9.1. Records relevant to administering this Procedure will be maintained for periods as specified below:

9.1.1. Data Subjects Rights Requests (DSRR)

The retention period for DSRRs, including the Data Subject Rights Request Form, related correspondences, and proof of legal authority to act on the data subject's behalf (if any) will be two years after the DSRR has been closed.

9.1.2. Data Subject Right Request Log

The log will be kept for audit, legal and accountability purposes. However, identifiers from each record, i.e., the name and contact details of the data subject will be deleted after a period of seven years from when the DSRR has been closed.

9.1.3. Abandoned DSRRs

The retention period for abandoned DSRRs will be three months after the last action related to the DSRR.

10. Complaints

10.1. If a data subject is dissatisfied with the way **Moroil** has dealt with his/ her request, the latter can make a complaint by contacting the **DPO** in writing.

10.2. The **DPO** will handle complaints received from all stakeholders concerned regarding data protection and will coordinate with relevant departments for investigation and managing responses.

10.3. When a complaint is received, the **DPO** will acknowledge receipt within two working days. The acknowledgement should contain information that the complaint has been received and is under review. Further, the data subject will be informed that a response will be provided within one calendar month.

10.4. Once the complaint has been acknowledged, the next step for the **DPO** will be to gather information about the complaint. This may involve requesting additional information from the data subject or conducting an internal investigation together with relevant departments to gather more details.

10.5. If the investigation is complex and will take time, the **DPO** will inform the data subject of any delay within one month of receipt of the complaint and must provide a reasonable estimate for the time (not exceeding one additional month) within which a response will be provided.

10.6. After the investigation is complete, **DPO** will respond to the data subject with the findings of the investigation. If an issue or any data protection violation is found, steps should be taken to correct the issue or violation and prevent it from happening again in the future. If no issue/violation is found, the data subject will be informed of this and provided with an explanation.

10.7. A record of all complaints and the steps taken to resolve them will be kept. This record can be used to identify patterns and trends in complaints and to track the effectiveness of the complaint-handling process.

10.8. If the data subject is still unhappy with the response that was provided, he/she can also file a complaint to the Data Protection Office.

11. Compliance, Monitoring and Review

11.1. The overall responsibility for ensuring compliance with the requirements of the related legislation in relation to processing subject access rights requests at **Moroil** rests with the **DPO**.

11.2. Non-compliance with this Procedure may result in disciplinary action and any exceptions to this Procedure are to be reported to the **DPO** for approval by the Managing Director.

11.3. Behaving in a manner contrary to what is contained in the Procedure will constitute a violation or breach which may be referred to relevant disciplinary processes.

12. Glossary of Abbreviations and Definitions

This section includes definitions for all terms used within this Procedure, including acronyms where applicable.

TERM	DEFINITION
Anonymisation	The process in which personal data is turned into anonymous information namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.
Consent	Any freely given, specific and informed expression of the wishes of the data subject, by which the data subject agrees to the processing of personal data relating to him or her which is in line with the requirements of the Mauritius Data Protection Act 2017.
Controller	A person who alone or jointly with others, determines the purposes and means of which personal data is to be processed, regardless of whether or not such data is processed by such person or agent on that person's behalf.
Data Protection Act 2017 (**DPA**)	The Act that regulates the protection of personal data in Mauritius.
Data Protection Office	The supervisory authority in Mauritius tasked to supervise compliance with the Mauritius **DPA**.
Data Protection Officer (DPO)	A person appointed by **Moroil** who will independently ensure that personal data is processed in a correct and lawful manner and who will ensure the **Moroil's** compliance with the Mauritius Data Protection Act 2017.
Data subject	An individual who is the subject of personal data such as an employee, customer, supplier, contractor, consultant, shareholder, board member, or director amongst others.
Direct marketing	Directly reaching a market, customers or potential customers on a personal basis or mass media basis and includes but is not limited to attempting to locate, contact, offer and make incentives to consumers, through communication mediums such as social media platforms (Facebook, LinkedIn), WhatsApp phone calls, private meetings and other mass marketing forms.

Employees	Any permanent employees (whether full-time or part-time), directors, executives, fixed term or temporary staff members, agents, consultants, seconded, home-based, casual and agency staff, volunteers and interns of **Moroil**.
Personal data	Information relating to an identifiable individual such as identification number, name, marital status, government-issued identification number, email address, personal telephone number, picture, one or more factors specific to the individual's physical, physiological, mental, economic, cultural or social identity amongst others.
Processing	Any operation or set of operations performed on personal data whether or not by automated means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	A person who processes data on behalf of the controller.
Sensitive personal data	Personal data relating to a data subject which reveals his or her racial or ethnic origin, political opinions, religious beliefs or philosophical beliefs, membership of a trade union, physical or mental health or condition, sexual orientation, practices or preferences, genetic data or biometric dadta uniquely identifying him, and the commission or alleged commission of an offence by him or any proceedings for any offence committed or alleged to have been committed by him or her, the disposal of such proceedings, or the sentence of any court in such proceedings and such other personal data as the Commissioner may determine to be sensitive personal data.

Appendix A: Data Subject Rights Request (DSRR) Form

Each of the rights listed below may be exercised by submitting this request to the **DPO** at the following email address: dpo@moroil.mu. Please complete in block letters and tick "X" where necessary.

Request will be processed upon positive identification and submission of the required documents to **Moroil**.

Please complete in block letters and tick as appropriate. Fields marked with * are required for the application to be processed.

Request being made in person: ☐	**Proxy:** ☐ *(in case of proxy, consent of the data subject is required to be attached to this request)*

With regard to:			
Right of Access	☐	Right to Withdraw Consent	☐
Right of Rectification	☐	Right to Erasure	☐
Right to Object	☐	Right to Restriction to Processing	☐
Right to Automated Individual Decision-Making	☐		

Further description of the request

Please describe your request in more details, include reason for the request and any details to help us understand and better respond to you. E.g., details of what processing to restrict or what personal data to be erased.

Data Subject's Data

Title	Mr ☐	Mrs ☐	Miss ☐
Name			
Current address			
Contact number			
Email address			

Proxy Details

Please state your relationship with the data subject (e.g., parent, legal guardian or solicitor)			
Title	Mr ☐	Mrs ☐	Miss ☐
Name			
Current Address			
Contact Number			
Email Address			

Preferred way of feedback on the request*:

☐ By email **☐ In writing** **☐ Other (please mention):** Click or tap here to enter text.

Signature: **Date:**

For Office Use:

The request is a valid one and the identity of the requester has been confirmed:

☐ Yes ☐ No

Date: Signature: