[Letterhead of MSCL]

| Identifier: | Version: | Effective Date: | Data Privacy Policy |
|---|---|---|---|
| MSCL-COM – POL-001 | V0 | 15/02/2019 | |
| Original Date: YYYY/MM/DY | 31/01/2019 | | |
| Document Owner: | MANAGER- BUSINESS ANALYTICS | | |

MSCL
The Medical and Surgical Centre Limited

## MSCL – Compliance

# DATA PRIVACY POLICY

## Document Revision History

| Revision Number | Revision Date | Summary of Changes | Approved by | Next Review Date |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |

## Document Review

This document requires following approvals:

| Title | Date | Signature | Name |
|---|---|---|---|
| *Head of HR* | *28/01/2019* | | *Clive Chung* |
| *Chief Operating Officer* | *31/01/2019* | | *Claire Wanquet/Olivier Schmitt* |

## Document Approval

This document requires following approvals:

| Title | Date | Signature | Name |
|---|---|---|---|
| *Chief Executive Officer* | *31/09/2019* | | *Olivier Schmitt* |
| | | | |

PLEASE MAKE SURE THAT THIS IS THE CURRENT VERSION BEFORE USE.

ONCE PRINTED, THIS IS AN UNCONTROLLED DOCUMENT.

| | |
|---|---|
| **Purpose** | This policy defines requirements to help ensure compliance with data privacy laws and regulations applicable to MSCL regarding collection, storage, use, transmission, disclosure to third parties and retention of personal information and sensitive personal information |
| **Scope** | This policy is for employees to maintain privacy of personal information held in physical files or in electronic form for patients and employees |
| **Responsibility** | MSCL Data Protection officer |
| **Definitions** | Refer to section 5 glossary (pg18) |
| **Links to other Policies/Documents** | Personal Data Breach Policy |
| **References** | http://dataprotection.govmu.org<br>https://eugdpr.org/ |
| **Training** | All MSCL employees |
| **Distribution** | All MSCL employees |

# Contents

# 1. Introduction

It is the policy of The Medical and Surgical Centre Limited (hereafter referred to as 'MSCL), to ensure that all its employees maintain privacy of personal information held in physical files or in electronic form. MSCL regards the lawful and correct treatment of personal information as very important and undertakes to maintain the confidentiality of the persons to whom the information relates.

## 1.1. Purpose

This policy defines requirements to help ensure compliance with data privacy laws and regulations applicable to MSCL regarding collection, storage, use, transmission, disclosure to third parties and retention of personal information and sensitive personal information.

## 1.2. Objective

The main objectives of the data privacy policy are to establish the principles and practices by which:

- All of the personal information in custody of MSCL is adequately protected against threats and the security of the personal information is maintained.
- Employees of MSCL are made fully aware of the contractual, statutory or regulatory implications of any privacy breaches.
- The use of personal information is limited to the identified business purposes for which it is collected.
- MSCL creates an awareness of privacy requirements such that these become an integral part of the day to day operation of every employee and ensure that all employees understand the importance of privacy practices and their responsibilities for maintaining privacy.
- All the employees are made aware of the processes that need to be followed for collection, lawful usage, disclosure/ transfer, retention, archival and disposal of personal information.
- All third parties collecting, storing and processing personal information on behalf of MSCL are held accountable to provide adequate data protection.
- Applicable regulations and contracts regarding the maintenance of privacy, protection and cross border transfer of personal information are adhered to.

## 1.3. Applicability

This policy is applicable to employees, contractors, vendors, interns, customers, and business partners of MSCL who may receive personal information, have access to personal information collected or processed by or on behalf of MSCL, or who provide information to MSCL.
This policy covers the treatment of personal information gathered and used by MSCL for lawful business purposes. This policy also covers the personal information shared with authorised third parties and that third parties share with MSCL.

## 1.4. Ownership

The policy is sponsored by the Data Protection Officer (DPO). The DPO is responsible for maintaining the document and for providing clarifications pertaining to the content.

### 1.5. Extent of compliance

Each policy statement is worded to indicate the extent to which compliance is required. Instances where 'must' or 'should' are used indicate mandatory compliance and non-compliance requires an approved exception. Statements where 'may' is used denote recommendations where compliance is optional but recommended.

### 1.6. Compliance monitoring

Compliance with the policy is required at all times. To allow for flexibility, the following two types of compliance activities may be performed to prevent and detect non-adherence:

- Internal verifications: The DPO must ensure that MSCL is compliant with the DPA 2017 and GDPR. For successful monitoring, the DPO may carry out ad-hoc verifications or may use any other means he/she deems fit, to ensure that the personal data of the employees and clients of MSCL is being processed in a lawful manner. The DPO must ensure that a record of the checks carried out is kept and is made available to any authorized party, as and when may be required.
- The Cluster DPO within each cluster can perform ad-hoc verifications of business units within the cluster to assess the extent of compliance with the requirements of this policy. Instances of non-compliance are reported to the Group DPO.
- Independent verifications: The Internal Audit may perform audits to detect instances of non-compliance and exceptions, which are reported to the Audit and Risk Management Committee.

### 1.7. Communication

The DPO is responsible for communicating the policy to relevant stakeholders, including new versions following revisions to the content.

### 1.8. Revision and update

The contents of this policy must be reviewed at least once every year and updated accordingly in line with changes in privacy laws and regulations and the business environment.

# 2. Policy statements

This section sets out the data privacy principles which MSCL is required to abide by. The principles have been defined to provide guidelines for the acceptable collection, use, disclosure and any other form of processing performed on the personal information of data subjects.

## 2.1. Management

- A privacy organisation must be defined for governance of data privacy initiatives at the level of MSCL. Refer to Appendix A for an overview of the privacy organisation structure and the roles and responsibilities of the Board of Directors, the Group DPO, MSCL DPO and the DPO Support Team.
- MSCL should appoint a DPO to process complaints and requests for personal information from data subjects.
- The MSCL DPO must investigate and report complaints and data breaches to the competent Supervisory Authorities and reply to any requests for information from data subjects. The MSCL DPO should notify the Group DPO of any data breaches.
- MSCL should establish procedures for the identification and classification of personal information.
- The Employee Privacy Policy Notice should be communicated to all employees.
- Regular awareness sessions and targeted training on data processing activities should be provided to ensure that all personnel involved in the processing of personal information are knowledgeable of the principles set out in the MSCL - Data Privacy Policy
- MSCL should establish disciplinary and remedial actions for violations of the MSCL - Data Privacy Policy across all of its subsidiaries which process personal data.
- Changes or updates to the MSCL - Data Privacy Policy should be communicated by the DPO to all personnel of MSCL when the changes become effective.
- MSCL should establish procedures for performing mandatory registration with regulatory bodies. As per the DPA 2017, a DPO must be appointed for each entity that processes personal information, including for clients, vendors and employees.

## 2.2. Collection of personal information

- The collection of personal information should be limited to the minimum requirement for lawful business purposes, namely:
  - Consent i.e. the data subject has given clear consent to process their personal information for a specific purpose
  - Contract i.e. the processing is necessary for performance of a contract MSCL has with the data subject, or the data subject has requested MSCL to take specific steps before entering into a contract
  - Legal obligation i.e. the processing is necessary for MSCL to comply with governing law
  - Vital interest i.e. the processing is required to save the data subject's life
  - Public task i.e. the processing is necessary for MSCL in the public interest or official functions and the task or function has a clear basis in law
  - Legitimate interest i.e. processing is necessary for the legitimate interest of MSCL or the legitimate interest of a third party unless there is reason to protect the data subject's personal information which overrides legitimate interest.
- Methods of collecting personal information should be reviewed by management to ensure that personal information is obtained:
  - Fairly, without intimidation or deception, and
  - Lawfully, adhering to laws and regulations relating to the collection of personal information.
- Management should satisfy itself that third parties from whom personal information is collected and with whom personal information is shared:

- Use fair and lawful information collection methods, and
- Comply with the MSCL Data Privacy Policy and their contractual obligations with respect to the collection, use and transfer of personal information on behalf of MSCL.

### 2.3. Data flow management

- MSCL must identify all the processing activities that involve processing of personal information. Processing activities include the collection, handling, disclosure, storage and disposal of data relating to personal information.
- Following the identification of the processing activities, MSCL must document a record of processing activities (RoPA) containing the following elements at a minimum:
  - The name and contact details of the organisation and the DPOs (Group DPO and MSCL DPO).
  - The purposes of the processing activity.
  - A description of the categories of data subjects and of the categories of data related to personal information.
  - The lawful basis for processing (as defined in section 4.2).
  - Applicability i.e. whether the processing falls under the scope of GDPR or Mauritius DPA 2017 or both
  - The categories of recipients to whom the personal information have been or will be disclosed.
  - Where applicable, transfers of personal information to a third country or an international organisation, and the documentation of safeguards implemented during the transfer.
  - The retention period of the data involved.
  - A general description of the technical and organisational security measures
- The RoPA should be documented in enough detail so as to provide a complete overview of the flow of data related to personal information within a processing activity. Refer to Appendix B for a recommended structure of the RoPA.

### 2.4. Risk management

- MSCL must perform a privacy risk assessment on a periodic basis to identify the risks associated with processing activities performed on data relating to personal information. The assessment should take into consideration the following criteria:
  - Impact/ severity of the risk based on level of identification of personal information and prejudicial effect of the impact.
  - Likelihood of materialisation of the risk.
- The criteria above are combined to obtain the risk level of the processing activities. Refer to Appendix C for a risk rating scales to be used for assessing the impact and likelihood of risks associated with processing activities.
- The risk rating constituting low, medium and high risk is outlined in Appendix C.
- For all high-risk processing activities identified following the privacy risk assessment, MSCL must perform a data privacy impact assessment (DPIA). A DPIA must also be performed in the following instances:
  - Processing activities that involve tracking individuals' online behaviours, including through cookies.
  - Processing activities which could result in a risk of physical harm in the event of a security breach.
  - If there is a change to the nature, scope, context or purposes of the processing activities, including events that significantly change the privacy environment of the company.
  - If MSCL is considering implementing new processing activities around personal information or special categories of personal information.
- MSCL must ensure that the DPIA is documented and contains the following information:
  - Description of the nature, scope, context and purposes of processing;

  - Identification of existing measures that are in place for the mitigation of risks associated with the processing activities, including frequency of control, control owner, details of who performs the controls and who reviews the controls;
  - Assessment of whether the existing measures effectively mitigate the risks associated with the processing activities as well as residual risk acceptance level;
  - Assessment of whether additional measures need to be implemented to mitigate the risks associated with processing activities, including responsible party for implementation, deadline for implementation, additional budget required.
  - Consultation with the Supervisory Authority or data subjects, if any was performed.
- MSCL must document the outcome of the DPIA, including any divergence of opinion with the Group DPO and/or individuals consulted. Following completion of the DPIA, it is signed off and retained for regulatory reporting purposes.
- Where MSCL cannot effectively mitigate high risks associated with processing activities, guidance from the Group DPO and/or the Supervisory Authority will be sought. Guidance on how to conduct a DPIA is annexed under Appendix D.
- Refer to Appendix D for the template for the documentation of the Privacy Risk Assessment and the DPIA.
- The DPIA should be maintained and revisited as necessary, and kept in a format that can be shared with the Supervisory Authority upon request.

2.5. **Notice**

- Appropriate notice should be provided to data subjects at the time personal information is collected. Refer to Appendix E for a template of the data privacy notice to the employees of MSCL.
- The privacy notice or policies and other statements to which they are linked should provide as full information as is reasonable in the circumstances to inform a data subject on how their personal information will be used so that the processing by MSCL is fair, transparent and lawful. The following aspects should be considered in the documentation of a notice:
  - Purpose for the processing and the legal basis for the processing;
  - The legitimate interest of MSCL or of any third party involved;
  - Categories of personal information;
  - Intended recipients of personal information;
  - Details of transfers to third parties and safeguards in place;
  - Retention period or criteria for the determination of the retention period;
  - The existence of data subject rights;
  - Existence of the right to withdraw consent at any time and consequences of withholding or withdrawing consent to the collection, use and disclosure of personal information for identified purposes;
  - Process for an individual to view and update their personal information records, request the erasure or restriction of their personal information or object to the processing of their personal information;
  - The right to lodge a complaint with a Supervisory Authority;
  - Whether the provision of personal information is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal information;
  - The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences of such processing for the data subject;
  - Contact information of MSCL and any other relevant company of the CIEL Group collecting personal information.
- Data subjects should be provided a Privacy Notice in case any new purpose is identified for using or disclosing personal information before such information is used for purposes not previously identified.

2.6. **Consent**

- Where consent is determined to be the lawful basis for processing, explicit consent should be obtained from data subjects at the time of collection of personal information or as soon as practical thereafter.
- Consent should be obtained from data subjects for the collection, use and disclosure of personal information, including sensitive personal information, when processing the personal information other than for the purpose defined in the agreement with data subjects, unless a law or regulation specifically requires or allows otherwise. MSCL obtaining the consent must keep records to demonstrate what the data subject has consented to, including what they were told, and when and how they provided consent.
- Consent must also be obtained based on the following criteria:
  - Unambiguous: data subjects need to easily understand what they are signing up for.
  - Unbundled: consent requests must be separate from other terms and conditions. Consent should not be a precondition of signing up to a service unless necessary for that service.
  - Active opt-in: MSCL must make available unticked opt-in boxes or similar active opt-in methods.
  - Granular: MSCL must give granular options to consent separately for different purposes;
  - Named: MSCL must name the relevant legal entities and any third parties who will be relying on consent.
  - Retractable: data subjects must be made aware that have the right to withdraw their consent at any time, and MSCL clearly details how data subjects can to do this. It should be as easy to withdraw as it was to give consent.
- Consent should be obtained from data subjects before their personal information is processed for purposes not previously identified.
- Appropriate consent should be obtained from data subjects before their personal information is transferred to or from information processing systems.

2.7. **Limiting use, disclosure and retention**

- Personal information should not be used or disclosed for purposes other than those for which it was collected, except in the following instances:
  - The new purpose is compatible with the original purpose
  - Consent is obtained from the data subject
  - There is a clear legal provision requiring or allowing the new processing in the public interest.
- Personal information retention should be only for the duration necessary to fulfil the identified lawful business purposes or as prescribed by law.
- MSCL must develop guidelines and procedures for the retention and disposal of personal information. These shall address minimum and maximum retention periods according to business/legal requirements, modes of storage and disposal methods amongst others.
- Upon the expiration of identified lawful business purposes, withdrawal of consent or a request to be forgotten, MSCL should either securely erase or anonymise the data subjects' personal information. Data is anonymised to prevent unique identification of an individual.

2.8. **Data subject requests**

- There are several instances whereby MSCL should be in a position to respond to requests from data subjects as follows:
  - Access request: MSCL should be able to provide information about personal information of the data subject being processed by the company and its third-parties/ vendors. Data subject may request a copy of their personal information which is being processed.
  - Rectification request: data subjects may require their personal information to be updated or made more complete and accurate.
  - Erasure request: data subjects may require their personal information to be erased from MSCL's systems and archives as well as data held by third-parties/ vendors.

  - Consent withdrawal request: data subjects may revoke consent previously provided at any moment.
  - Restriction of processing request: data subjects may request that processing of their personal information be suspended for a temporary period.
  - Objection of processing request: data subjects may object to the processing of their personal information.
  - Portability request: data subjects may request for their personal information to be transferred to a different data controller or processor.
  - Objection to automated decision making request: data subjects may request not to be subject to automated decision making.
- MSCL should establish processes and forms to respond to requests from the data subject.
- The identity of data subjects requesting access to their personal information should be reasonably verified before providing access to such information. For instance, this could be done by requesting for a copy of the requester's national ID card. The principles set out in this policy document are adhered to in handling the personal information collected as part of the verification process.
- A response should be given to data subjects requesting access to their personal information in an accessible form, within a defined period from receipt of complaint/ request as prescribed by law.
- Data subjects should be notified, in writing of the reason for any denial of requests for access to personal information to the extent required by applicable law.
- MSCL must respond to the data subject requests within a maximum of 30 days of the receipt of the request.

### 2.9. Disclosure to third parties and outward transfers

- Personal information should be disclosed to third parties only for identified lawful business purposes and after obtaining appropriate consent from the data subjects, unless a law or regulation allows or requires otherwise.
- Where reasonably possible, MSCL should ensure that the following contractual agreements are implemented with third parties collecting, storing or processing personal information on behalf of MSCL:
  - Signed agreements to protect personal information consistent with MSCL's Data Privacy Policy and information security practices or implemented measures as prescribed by law. The agreements must include terms that define:
  - the role of each contracting authority as controller or processor, the roles of the controller and the processor, nature and purpose of processing, duration of processing and categories of personal information processed. The agreements should also hold the third parties accountable for the lawful processing of the personal information provided by MSCL as mandated by the applicable data privacy laws.
  - Signed non-disclosure agreements or confidentiality agreements which includes privacy clauses in the contract.
- MSCL should establish procedures to ensure that all contracted parties meet the terms of their agreements as set out above to protect the personal information.
- Personal information may only be transferred across geographies where MSCL operate, or where MSCL has outsourced data processing activities if any of the following conditions apply:
  - MSCL has provided the Commissioner proof of appropriate safeguards with respect to the protection of personal information, as required by the Mauritius DPA 2017.
  - The individual has given explicit consent to the transfer of information (if consent is the lawful basis), after having been informed of the possible risks of the transfer.
  - The transfer is necessary for the performance of a contract between the individual and MSCL, or the implementation of pre-contractual measures taken in response to the individual's request.
  - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between MSCL and a third party.

  - The transfer is necessary or legally required on important public interest grounds or for the establishment, exercise or defence of legal claims.
  - The transfer is required by law.
  - The transfer is necessary in order to protect the vital interests of the data subject.
  - The transfer is made under a data transfer agreement between MSCL and the data processors involved.
  - The transfer is otherwise legitimised by applicable law.
- Remedial action should be taken in response to misuse or unauthorised disclosure of personal information by a third party collecting, storing or processing personal information on behalf of MSCL and its business units.

### 2.10. Security practices for privacy

- In line with the risk management framework, MSCL should assess the relevance of implementing a formal information security management system which covers the following aspects:
  - Security policies
  - Organisation of information security
  - Asset management
  - Access management
  - Communications security
  - Physical & environmental security
  - Operations security
  - Cryptography
  - Supplier relationship
  - System acquisition, development and maintenance
  - Information security aspects of business continuity management
  - Information security incident management
  - Human resource security
  - Compliance
- The information security policies and procedures of MSCL should be documented and implemented to ensure reasonable security for personal information collected, stored, used, transferred and disposed by MSCL.
- The assessment performed by each business unit should be documented.

### 2.11. Breach management

- MSCL has implemented a privacy breach management process which is fully set out in the "Personal Data Breach Policy" which aims at monitoring, identifying and responding to data privacy breaches within the timeframes imposed by the privacy laws. The process should address the following:
  - Responsibilities for identifying, monitoring, classifying, escalating and resolving of privacy incidents.
  - Requirements, timeframes and responsibilities of notifying the breach to the Supervisory Authority.
  - Requirements and responsibilities for notifying the Supervisory Authority within 72 hours of identifying the breach and data subjects, where applicable.
  - Means and channels of notification to the Supervisory Authority and data subjects, where applicable.
- MSCL should maintain an inventory of all privacy breaches for communication to the Supervisory Authority upon requests and to facilitate response to data subject requests. The inventory should be documented in a privacy breach register containing the following at a minimum:
  - Date of breach occurrence (or an estimate)
  - Date of breach identification
  - Location of the breach
  - Third parties involved (e.g. data processor)
  - Type of breach

- Description of the breach
- Suspected cause of the breach
- Description of personal information affected (nature and content)
- Type of data subjects affected (e.g. adult or children)
- Number of data subjects affected (or an estimate)
- Measures that had been implemented to prevent data breach
- Severity of breach
- Remedial action taken to address the breach
- Date of notification to the supervisory authority
- Date of notification to data subjects (where applicable)

Refer to Appendix F for a template of the privacy breach register.

- MSCL must use a methodology for assessing the severity of the breach by taking into account the type of data, ease of identification of data subject and the receiver of the breach information. The severity of the breach is measured by combining the three factors. Refer to Appendix G for the privacy breach severity assessment methodology.
- When determining the severity of the breach, MSCL should apply and document its own judgment to override the severity rating when in doubt of the potential risk resulting from the breach.
- The MSCL DPO must develop privacy breach notification forms that will be used by MSCL and the business units to notify the Supervisory Authority and the data subjects.
- The following details must be included in the form to notify data privacy breaches to the Supervisory Authority:
  - Contact details of MSCL DPO – including name, job title, email, phone number, physical address
  - Date of breach occurrence or an approximate date
  - Date of breach identification
  - Description of the breach
  - Suspected cause of breach
  - Nature and content of personal information breached
  - Measures that had been implemented to prevent data breach
  - Third-parties involved
  - Approximate number of data subjects impacted
  - Type of data subjects impacted (e.g. child or adult)
  - Possible consequences of the breach of the data subjects
  - Measures implemented to minimise impact of the data breach
  - Notification to data subjects, if applicable.
- The following details must be included in the form to notify data privacy breaches to the data subjects:
  - Contact details of MSCL DPO – including name, job title, email, phone number, physical address
  - Date of breach occurrence or an approximate date
  - Date of breach identification
  - Description of the breach
  - Suspected cause of the breach
  - Nature and content of personal information breached
  - Measures that had been implemented to prevent data breach
  - Possible consequences of the breach of the data subjects
  - Measures implemented to minimise impact of the data breach

2.12. **Quality of personal information**

- MSCL should perform additional validation procedures to ensure that personal information collected is accurate and complete for the business purposes for which it is to be used.

- MSCL should ensure that personal information collected is relevant to the business purposes for which it is to be used.

2.13. **Privacy monitoring and enforcement**

- MSCL should establish procedures for recording and responding to complaints/ grievances registered by data subjects.
- Each complaint regarding privacy practices registered by data subjects should be validated, responses documented and communicated to the individual.
- Annual privacy compliance review should be performed by MSCL for identified business processes and their supporting applications.
- A record should be maintained of non-compliances identified in the annual privacy reviews. MSCL should ensure that disciplinary and remedial actions identified are followed through.
  Corrective and disciplinary measures should be initiated and tracked to closure.
- Procedures should be established to monitor the effectiveness of controls for personal information and for ensuring corrective actions, as required.
- Any conflicts or disagreements relating to the requirements under this policy or associated privacy practices should be referred to the Group DPO for resolution.

2.14. **Personally Identifiable Information (PII) of employees within MSCL**

- MSCL may process the following types of sensitive and non-sensitive PII relating to employees:
  - Names, addresses, telephone numbers and other personal contact details.
  - Derived information, such as notes taken during an interview.
  - Gender, date of birth, physical or mental health or condition.
  - Marital status, next of kin.
  - Insurance details and trade union membership.
  - Personnel records including training, appraisal, performance and disciplinary information
  - Bank details, salary, bonus, benefits and pension details and other financial information.
  - Criminal offences committed (or allegedly committed) including any proceedings and sentencing in relation to any such criminal offence.

2.15. **Staff data processing activities**

- MSCL may undertake a number of lawful processing activities with an individual employee's personal information in the context of employment as fully set out under MSCL's Privacy Notice to Employees, a copy of which has been issued to all employees of MSCL including, but not limited to:
  - Salary, benefits and pensions administration.
  - Health and safety records and management.
  - Security vetting, criminal records checks and credit checks and clearances (where applicable and allowed by law).
  - Confirming information on résumés, CVs and covering letters, providing reference letters and performing reference checks.
  - Training and appraisal, including performance evaluation and disciplinary records.
  - Staff management and promotions.
  - Succession planning.
  - Any potential change of control of a group company, or any potential transfer of employment relating to a business transfer or change of service provider.
  - Other disclosures required in the context of staff employment.

- Promoting or marketing of MSCL, its products or services.
- Provision of staff or business contact information to customers and agencies in the course of the provision of services offered by MSCL.
- CCTV monitoring for security reasons.
- Compliance with applicable procedures, laws, regulations, including any related investigations to ensure compliance or of any potential breaches.
- Establishing, exercising or defending legal rights of MSCL and its business units.
- Disclosures to other companies with MSCL, including companies in other countries to the extent permitted by law, including for the following purposes: as required in connection with the duties of the employee; legal compliance; audit; group level management; in connection with the fulfilment of customer and partner contracts.
- Any other reasonable purposes in connection with an individual's employment or engagement by MSCL or one of its business units.
- Providing and managing use of services provided by third parties, such as company provided mobile devices, company credit cards and company cars and billing for such services.
- MSCL also collect and process personal information about a person's next of kin so they can be contacted in an emergency or in connection with use of a company car provided by MSCL or its subsidiaries. Their personal information will also be processed in accordance with the data protection laws and as described in the policy.
- In order to fulfil the purposes set out above, MSCL may disclose personal information to contractors and suppliers that provide services to MSCL and who may assist in the processing activities set out above provided that contractual agreements as defined in section 4.9 have been executed.
- MSCL may disclose personal information to law enforcement agencies, regulatory bodies, government agencies and other third parties as required by law or for administration/taxation purposes, to the extent local law allows and requires.

- If MSCL decides to process employee personal information other than for processing activities that are reasonably expected to be performed during the course of employment, it should obtain consent of the concerned employees prior to the processing activity. These include for marketing and profiling reasons.
- MSCL may disclose personal information to third parties for the purposes of establishing and managing employment relationship. For example, MSCL may disclose some personal information to:
  - benefits providers (for example, pension and insurance providers);
  - payroll and data processing suppliers and other service providers who assist in establishing or managing employment relationship;
  - insurance claims and medical related service providers; and
  - parties requesting an employment reference.
- MSCL should take appropriate measures to ensure that its contractors and suppliers also process personal information in a compliant way and such measures may include a data processing agreement.
- MSCL may transfer personal information to other group companies, partners, suppliers, law enforcement agencies and to other organisations in all cases that are located outside of the country where the employee is based for the purposes of:
  - HR administration (for example, staff recruitment).
  - Payroll processing for employees working outside the country where they are based.
  - Employee relocation.
  - Security clearances.
  - Visa applications.
  - Taxation and registrations for employees working outside the country where they are based.
  - Fulfilling the legal requirements of MSCL.
  - Fulfilling customer contracts for the provision of services offered by MSCL.
  - Overseas legal proceedings.

- Outsourcing functions of MSCL.

2.16. **Sharing of personal information within MSCL group**

- There are instances wherever subsidiaries within the group use the services of other subsidiaries, and these involves the transfer of personal data. Although the controllers that are part of the group may have a legitimate interest in sharing personal data for the provision of services or administrative tasks, mutual agreements must be established defining the responsibilities of each.

2.17. **Retention of records**

- MSCL has a statutory duty to keep certain records for a minimum period of time. In other cases, MSCL should not keep personal information for longer than is necessary or as may be required by applicable law. MSCL will develop guidelines and procedures for the retention and disposal of personal information.

2.18. **CCTV**

- Some of buildings and sites of MSCL use CCTV systems to monitor their exterior and interior 24 hours a day for security reasons. This data is recorded. Use of CCTV and recording of CCTV data is only carried in accordance with the approved guidelines of MSCL.
- MSCL should take reasonable efforts to inform individuals that the area is under electronic surveillance. This may be performed by the use of clear and legible notices placed at the entrances and areas of the building that are under surveillance. Refer to Appendix H for guidelines on the use of CCTV and recording of CCTV data.

2.19. **Use of fingerprints**

- MSCL collects fingerprints of employees for monitoring of attendance and/or for access control purposes. As per GDPR and Mauritius DPA 2017, personal data must be obtained fairly. MSCL must ensure that employees are fully aware of the implications of having their fingerprints taken before doing so. MSCL should explain the reasons for needing to collect fingerprints, and how the fingerprints and other personal data will be used and be kept safe. MSCL should respect the wishes of employees who object to fingerprinting and should provide alternative means for monitoring of attendance and access controls, such as cards. In cases where employees agree to the use of fingerprints for monitoring of attendance and/ or for control access purposes, MSCL must ensure that the explicit consent of the employees is obtained. Refer to Appendix I for the consent form for the use of fingerprints.

2.20. **Certification**

- MSCL may seek for certification from the Supervisory Authority or accredited certification bodies when these become available. Certification does not reduce the data protection responsibilities of but can allow for demonstration of compliance, in particular with regard to implementing technical and organisational measures. As data controllers, MSCL should familiarise itself with relevant schemes and take account of certifications, seals and marks when selecting their processors/ service providers.

# 3. Glossary

| Term | Definition |
|---|---|
| Anonymise | To process a collection of personal information such that a natural person cannot be identified on the basis of the output collection of data or information |
| Consent | Any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to the data subject. |
| Controller | The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal information; where the purposes and means of such processing are determined by law, the controller or the specific criteria for its nomination may be provided for law. |
| Cookie | A small text file stored on a data subject's machine that may later be retrieved by a web server from the machine. Cookies allow web servers to keep track of the end user's browser activities, and connect individual web requests into a session. Cookies can also be used to prevent users from having to be authorised for every password protected page they access during a session by recording that they have successfully supplied their user name and password already. |
| Data subject | A living individual about whom personal information is processed by or on behalf of MSCL. |
| Information security | Preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved. |
| Personal information of personally identifiable information (PII) | Any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person. |
| Privacy breach | A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed. |
| Processor | A natural or legal person, public authority, agency or other body which processes personal information on behalf of the controller. |
| Sensitive personal information | Special categories of personal information which include genetic data, and biometric data where processed to uniquely identify an individual. |
| Supervisory Authority | The national data protection authorities, empowered to enforce GDPR in their own member states. |

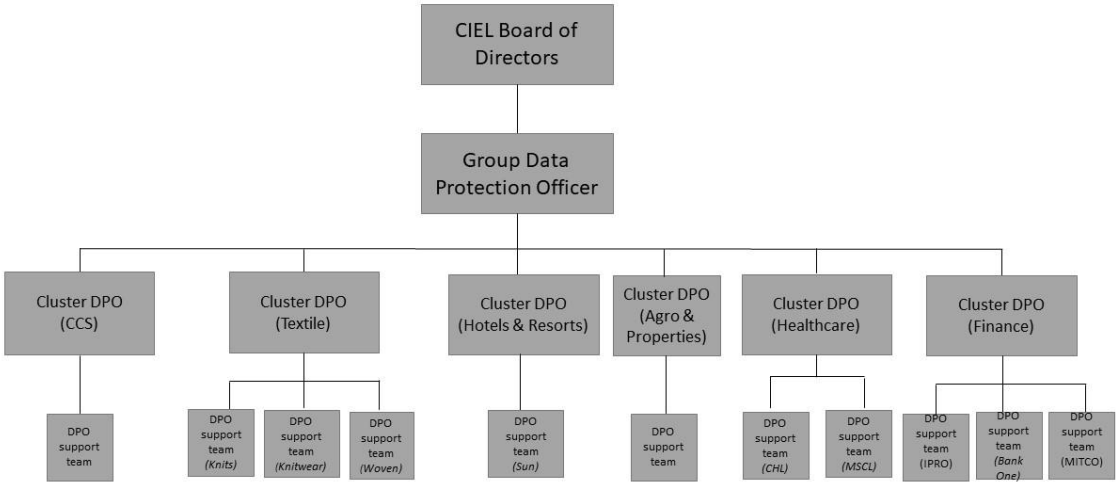
| Term | Definition |
|---|---|
| | For business units incorporated in Mauritius, the Supervisory Authority is the Mauritius Data Protection Office for Mauritius DPA 2017 and GDPR purposes. |
| Third party | All external parties – including without limitation contractors, interns, summer trainees, vendors, service providers and partners – who have access to MSCL's and its business units' information assets, information systems or who pass personal information from them. |

# 4. Appendices

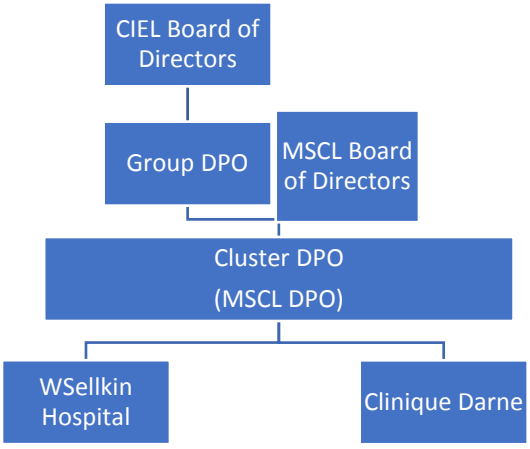
## Appendix A: Privacy organisation structure

The privacy organisation has been proposed keeping in mind that MSCL is part of CIEL Limited and operates under the Healthcare Cluster. Stakeholders and oversight from key business functions and senior leadership provides sustainable and practical guidance for the privacy framework.

**Privacy organisation structure**




*Regarding the healthcare Cluster, the following organisation structure will apply:*




**Roles and responsibilities**

Board of Directors:

The CIEL Board of Directors shall be responsible for data privacy across the Group whilst the MSCL Board of Directors shall be responsible to ensure compliance with data privacy laws across all subsidiaries and affiliates of

MSCL and relevant business units. The role of the Board of Directors is to channel resources and address organisational issues related to privacy.

The responsibilities of Board of Directors with regards to data privacy include the following:

- Review and approve Group Data Privacy Policies (Ciel Board of Directors) and MSCL Data Privacy Policies (MSCL Board of Directors).
- Establish a process for the enforcement of the various Data Privacy Policies.
- Ensure the implementation of a data privacy program that enables compliance with the Group Data Privacy Policies and MSCL Data Privacy Policies and applicable regulations with respect to data protection.
- Define processes to address grievances and handling complaints from data subjects with respect to their personal information held by CIEL/MSCL and its subsidiaries and business units.
- Determine the actions to be taken against grievances and information request cases presented by the Group DPO and Cluster DPO to the Board of Directors
- Review the findings from periodic privacy compliance reviews and sanction the implementation of corrective actions if applicable.
- Ensure that privacy impact assessments and measures to address privacy risks are aligned with the enterprise risk management framework.
- Monitor the data privacy program effectiveness.

Group Data Protection Officer

The role of Group Data Protection Officer (Group DPO) is to act as a central authority for the implementation and enforcement of CIEL privacy program. The Group DPO is required to advocate for the privacy program, articulate and communicate the organisation's privacy goals, and lead enforcement of the Group Data Privacy Policy. To achieve this, the appointed Group DPO should have the organisational credibility to facilitate decision making and resource allocation.

The Group DPO should:

- Be independent and free from conflicts of interest. As such, the Group DPO cannot hold a position within the organisation that leads him/her to determine the purposes and the means of the processing of personal information.
- Report to the highest authority within the organisation, in effect the Board of Directors.
- Have sufficient time and resources (financial, infrastructure and human) to fulfil his/her duty. This will be especially important if CIEL decides to appoint the Group DPO on a part-time basis or outsources the function.
- Have access to all functions within the organisation as and when necessary.
- Be provided with the required and continuous training to stay up to date on developments relating to data protection.
- Encourage each business unit to organise privacy awareness sessions for their employees. Refresher privacy awareness sessions must be given periodically to ensure that all employees are familiar with the requirements of privacy regulations. The frequency of the refresher privacy awareness sessions may vary depending on frequency of changes to current privacy requirements, emerging privacy requirements and turnover rate within MSCL. Awareness sessions must also be provided to all new joiners, for example as part of on-boarding procedures.
- Encourage the Cluster DPOs and their DPO Support Teams to undergo training on data privacy. The Cluster DPOs and the DPO Support Teams should receive adequate training, both as they assume their role in the data privacy program, and as the program evolves to address new developments in the business operations, data collection practices, supporting technology and services exchanged with external parties.
- Establish contact with appropriate supervisory authorities and governmental agencies related to data protection and privacy.

- Ensure that appropriate certification of the privacy practices is obtained and maintained.
- Support the Cluster DPOs and employees on Data Privacy Policy and organisational issues.
- Provide counsel, in consultation with the Legal Counsel, relating to privacy aspects of business contracts and partnerships including to the Board of Directors and Cluster DPOs.
- Conduct or coordinate data privacy audits.
- Establish procedures for disciplinary and remedial actions for Data Privacy Policy violations.
- Ensure that privacy impact assessments are undertaken to understand the risks to privacy raised by high risk processing activities.
- Ensure that an inventory is developed and maintained for personal information in CIEL and in each business unit.
- Provide inputs for privacy risk mitigation strategies.
- Define and communicate the privacy data breach response plan.
- Coordinate with the Cluster DPO to ensure that required documentation for compliance to data privacy laws and regulations, including the record of processing activities are properly maintained.
- Participate in audits.

Cluster Data Protection Officers (Cluster DPOs)

The Cluster Data Protection Officers (Cluster DPOs) will act as advocates for the Group data privacy program in their respective clusters. Situating the responsibility for the data privacy program at each cluster and across the organisation enables optimal resource placement and organisational awareness.

Each Cluster DPO should have the following competencies:

- Knowledge of national and applicable international data protection laws and practices and in-depth understanding of these laws.
- In-depth knowledge of the different business activities performed within each cluster.
- Sufficient understanding of the processing operations carried out within the cluster.
- Knowledge of the data security and data protection needs of the cluster.
- Knowledge of risk management applicable to cluster's context.
- Project management skills.

The Cluster DPOs should have similar attributes to the Group DPO and should report to the Group DPO and to the MSCL Board of Directors.

The responsibilities of Cluster Data Protection Officers include the following:

- Ensure the implementation and enforcement of controls arising out of the MSCL Data Privacy Policy across each business unit within their respective cluster.
- Maintain a cluster-wide view of business processes impacting privacy, and the nature, size and sensitivity of personal information held by the cluster.
- Provide guidance and information to business units within the cluster on their data protection obligations.
- Encourage each business unit within their respective cluster to organise privacy awareness sessions for their employees. The privacy awareness sessions should be designed with the following considerations:
    - Providing briefings, information and resources for employees to keep them apprised of current and emerging privacy requirements;
    - Providing employees with adequate guidance on identifying and appropriately handling data protection issues that may affect the performance of their job; and
    - Sensitising employees to the importance of data privacy to data subjects and the organisation.

  Refresher privacy awareness sessions must be given periodically to ensure that all employees are familiar with the requirements of privacy regulations. The frequency of the refresher privacy awareness sessions may vary depending on frequency of changes to current privacy requirements, emerging privacy requirements and

turnover rate within MSCL. Awareness sessions must also be provided to all new joiners, for example as part of on-boarding procedures.

- Encourage the DPO Support Team to undergo training on data privacy. The DPO Support Teams should receive adequate training, both as they assume their role in the data privacy program, and as the program evolves to address new developments in the business operations, data collection practices, supporting technology and services exchanged with external parties.
- Establish contact with appropriate supervisory authorities and governmental agencies related to data protection and privacy.
- Conduct or coordinate data privacy audits across business units within their respective cluster.
- Ensure that privacy impact assessments are undertaken by business units within their respective cluster to understand the risks to privacy raised by high risk processing activities.
- Ensure that an inventory is developed and maintained by business units within their respective cluster for personal information in CIEL and in each business unit.
- Communicate the MSCL's privacy data breach response plan (and such other policies and procedures) across their respective cluster.
- Coordinate with the DPO Support Team and other relevant stakeholders within their respective cluster to ensure that required documentation for compliance to data privacy laws and regulations, including the record of processing activities are properly maintained.

Business Unit Data Protection Officers (BU DPOs)

Each Business Unit Data Protection Office (BU DPO) shall ensure compliance with the Mauritius DPA 2017 and the EU-GDPR, as well as the Group Data Privacy Policy, within his Business Unit.

Each BU DPO should have the following competencies:

- Knowledge of national and applicable international data protection laws and practices.
- In-depth knowledge of the business activities performed within the business unit.
- In-depth understanding of the processing operations carried within the business unit.
- Knowledge of the data security and data protection needs of the business unit.
- Knowledge of risk management applicable to the business unit's context.
- Project management skills.

Over and above reporting to the Management of his BU, the BU DPO should have a reporting line to the Cluster DPO.

The responsibilities of each BU BPO include the following:

- Ensure the implementation and enforcement of controls arising out of the Group Data Privacy Policy across his business unit.
- Maintain a holistic view of business processes impacting privacy, and the nature, size and sensitivity of personal information held by his BU.
- Provide guidance and information on data protection obligations.
- Facilitate privacy awareness training for all employees.
- Maintain and update the personal information inventory, ensuring reconciliation with the information asset inventory.
- Perform quarterly review and update of the personal information inventory.
- Coordinate efforts for periodic privacy audits.
- Conduct privacy impact assessments for any high-risk processing activity.
- Ensure that privacy risk mitigation strategies are implemented, under the guidance of the Group and Cluster DPOs.
- Respond to data breach notifications as per the defined data breach response plan.

- Ensure that registrations and notifications are maintained and are up to date.
- Seek advice from the Group / Cluster DPOs on all pertinent data privacy matters.
- Maintain required documentation for compliance to data privacy laws and regulations, including the record of processing activities.
- Provide guidance on risk associated with processing operations and monitor the DPIA process.
- Ensure the appointment of a representative in the EU if such an appointment is required under the GDPR and communicate the details of the EU representative to the Group and Cluster DPO.
- Coordinate with the offices of governmental agencies and supervisory authorities during the investigation of a privacy complaint against the organisation.
- Handle requests for information made by individuals and third party agencies (including law enforcement agencies).

BU DPO Support Team

A DPO Support function comprising of one or more employees may be set up by each business unit within each cluster to provide assistance on data privacy matters to the DPO BU.

Members of the DPO Support team should have the following competencies:

- Knowledge of national and applicable international data protection laws and practices.
- In-depth knowledge of the business activities performed within the business unit.
- In-depth understanding of the processing operations carried within the business unit.
- Knowledge of the data security and data protection needs of the business unit.
- Knowledge of risk management applicable to the business unit's context.
- Project management skills.

The responsibilities of members of the DPO Support Team include the following:

- Support the BU DPO in the implementation and enforcement of controls arising out of the Mauritius DPA 2017, the EU-GDPR and the Group Data Privacy Policy.
- Maintain a view of business processes within the business unit impacting privacy, and the nature, size and sensitivity of personal information held by the business unit.
- Assist the BU DPO in facilitating privacy awareness training for all employees within the business unit.
- Maintain and update the personal information inventory for their business unit.
- Assist the BU DPO in conducting privacy impact assessments.

The DPO Support Team should report to the BU DPO.

# Appendix B: Proposed structure for the Record of Processing Activities (RoPA)

- The RoPA for MSCL can be documented in a spreadsheet using the template of the ROPA as published by the Data Protection Office is available on the following link: http://dataprotection.govmu.org/English/Pages/HomeDocuments.aspx

The ROPA should contain the following details:

- Topic:
  - Details of business function
  - Name of the processing activity
  - Sub-process name (if applicable)
- Personal data:
  - Details of whether personally identifiable information (PII) is being processed
  - Description and categories of PII
  - Description and special categories of PII
  - Origin of information
  - Comments
- Data subjects:
  - Categories of individuals
  - Approximate number of individuals concerned by the processing activity
- Details of processing:
  - Short description of the processing activities
  - Whether a data processor is involved
  - In case a data processor is involved, whether a formal agreement is in place
  - Details of the data controller i.e. which entity is the controller
  - Name and contact information of the controller
  - Purpose of the processing
  - Lawful basis for processing PII
  - Legitimate interests for the processing (if applicable)
  - Lawful basis for processing special categories of PII
  - Whether data minimisation is involved
- Applicability:
- Whether the processing falls under the scope of GDPR or Mauritius DPA 2017 or both
- Transfer:
  - Details of local recipients
  - Whether there is transfer of PII to a country outside of Mauritius
  - Details of foreign recipients
- Third-parties:
  - Whether there are third parties involved with the processing of PII, including location of the third parties
- Security measures:
  - General descriptions of security measures
  - Level of authorization required to access the PII
  - Storage, including country of storage for cloud services
- Retention period:
  - Intended retention period
  - Classification, identification and labelling of data
- Profiling:

    - Whether the PII is used for profiling
- Output of the processing activity
- Systems:
    - Concerned systems/ applications
    - Whether unstructured data is involved
- Disclosure:
    - Details of external entities to which PII may be disclosed
    - Reasons for disclosure
- Data privacy impact assessment (DPIA):
    - Whether DPIA is required
    - DPIA progress
    - DPIA reference

# Appendix C: Privacy risk assessment rating scales

The following scales must be used for assessing the impact and likelihood of risks associated with processing activities. Based on the scales, the risk rating will be categorised as follows:

| Risk | Score |
|---|---|
| High | 7-10 |
| Medium | 5-6 |
| Low | 2-4 |

- Rating scale for impact

| Impact | | | |
|---|---|---|---|
| Score | Rating | Level of identification of data subjects | Effect to individuals |
| 5 | Catastrophic | Identifying a data subject using their personal information appears to be extremely easy | Data subjects may encounter significant or irreversible consequences, which they may not be able to overcome |
| 4 | Major | Identifying a data subject using their personal information appears to be relatively easy | Data subjects may encounter significant consequences, which they should be able to overcome with serious difficulties |
| 3 | Moderate | Identifying a data subject using their personal information appears to be moderately difficult but is possible in certain cases | Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties |
| 2 | Minor | Identifying a data subject using their personal information appears to be extremely difficult | Data subjects may encounter a few inconveniences, which they will overcome without any problem |
| 1 | Insignificant | Identifying a data subject using their personal information appears to be virtually impossible | Data subjects either will not be affected |

- Rating scale for likelihood

| Likelihood | | | |
|---|---|---|---|
| Score | Rating | Occurrence in future | Occurrence in past |
| 5 | Expected | Very high, will be almost a routine feature every month within the immediate next year | Similar instances have commonly occurred every month in the past |
| 4 | Likely | High, may arise several times within the immediate next year | Similar instances have commonly occurred several times in the past year |
| 3 | Possible | Possible, may arise once or twice within the immediate next year | There have been 1 or 2 similar instances in the past |
| 2 | Unlikely | May occur once or twice between 2 (from now) to 5 years | Though not routinely, there have been similar instances in the last 2 to 5 years |
| 1 | Rare | Not likely, almost impossible to occur between 2 (from now) to 5 years | Similar instances have never occurred in the past |

# Appendix D: Template for documentation of Privacy Risk Assessment and DPIA

- Guidelines on how to conduct a Data Privacy Assessment and a DPIA together with the DPIA Form as published by the Data Protection Office is available on the following link: http://dataprotection.govmu.org/English/Pages/HomeDocuments.aspx

# Appendix E: Template of Employee Data Privacy Notice

The Medical and Surgical Centre Limited ("MSCL" or the "Company" or "we" or "us") collects, both in paper and electronic forms, and processes Personal Data relating to its employees ('employee(s)' or 'you') to manage the employment relationship. When we do, we are regulated as a 'data controller' of that Personal Data by the Data Protection Act 2017 (the "Act") or, where applicable, the European General Data Protection Regulations ("GDPR") (together the "Data Protection Laws").

The Company is committed to being transparent about how it processes its employees Personal Data and to meeting its data protection obligations under the Data Protection Laws.

For the purpose of this privacy statement ("Privacy Statement"), below are some definitions:

- "**Anonymise**" relates to "**Pseudonymisation**" as defined under the Act as the Processing of Personal Data in such a manner that the employee's Personal Data can no longer be attributed to the employee specifically 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 is not attributed to the employee;
- **"Biometric Data"** means any Personal Data relating to the physical, physiological or behavioural characteristics of an employee which allow his unique identification, including facial images or dactyloscopic data. For the purpose of this Privacy Statement, Biometric Data includes the employee's fingerprint;
- **"CIEL Group"** means collectively CIEL Limited, a public company listed on the stock exchange of Mauritius incorporated in Mauritius bearing Business Registration Number C06000717 and all of its subsidiaries and other investee companies which may or may not be controlled by CIEL Limited.
- "**Comply with a legal or regulatory obligation**" means Processing employee's Personal Data where it is necessary for compliance with a legal or regulatory obligation that we are subject to, as your employer;
- "**Consent**" means any freely given specific, informed and unambiguous indication of the wishes of an employee, either by a statement or a clear affirmative action, by which he signifies his agreement to Personal Data relating to him being processed;
- "**Direct Marketing**" means the communication of any advertising or marketing material which is directed to the employee;
- "**Legitimate Interest**" means the interest of our business in conducting and managing our business to enable us to manage our employment relationship with our employees and to comply with our legal and regulatory obligations under the Data Protection laws and other applicable laws. We make sure we consider and balance any potential impact on our employees (both positive and negative) and the overriding fundamental rights and freedoms of our employees before we process Personal Data of our employees for our Legitimate Interest. We do **not** use the Personal Data of our employees, unless we have their Consent or are otherwise required for the performance of our employment contract or as permitted to by law, if the fundamental rights and freedoms of our employees override our compelling Legitimate Interests to use the employee's Personal Data. The employees can obtain further information about how we assess our Legitimate Interest against any potential impact on the employee in respect of specific activities by contacting us;
- "**Personal Data**", or "personal information" means any information relating to the employee from which the employee can be identified. It does not include data where the employee's identity has been removed (anonymous data);
- "**Processing**" means any operation or set or operations which is performed on Personal Data or on 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, and erasure or destruction of data.
- **"Special Category of Data" or "Sensitive Data"** means Personal Data pertaining to the employee;s racial or ethnic origin; political opinion or adherence; religious or philosophical beliefs; membership of a trade union; physical or mental health or condition; sexual orientation, practices or preferences; genetic data or Biometric Data uniquely identifying the employee; the commission or alleged commission of an

offence by the employee; any proceedings for an offence committed or alleged to have been committed by the employee, the disposal of such proceedings or the sentence of any Court in the proceedings

- "**Third party**" means a natural or legal person or a public body other than the employee or us as the controller or a processor or a person who, under the direct authority of the controller or processor, is authorized to process your Personal Data;

We ask that each employee reads carefully this Privacy Notice as it contains important information on who we are, which types of Personal Data we collect about our employees, how and why we process, control and protect the Personal Data of our employees, and it tells the employees about their rights in relation to their Personal Data.

***IMPORTANT:***

***Except for certain information that is required by law, the employee's decision to provide Personal Data to us is voluntary. By signing and returning a duplicate of this Privacy Statement, the employee Consents that the Company processes and controls his Personal Data in accordance with this Privacy Notice and the Data Protection laws.***

***The employee has some obligations under his employment contract to provide us with his Personal Data for the purposes specified below.***

***If the employee does not wish to provide us with his Personal Data, or fails to provide the same, when requested, the employee will not be subject to adverse consequences. However, this may mean that the employee would be unable to exercise his legal rights as our employee. Also, please note that if the employee does not provide certain information, the Company may not be able to efficiently accomplish some or all of the purposes outlined in this Privacy Notice, in particular, we will not be able to manage the employment relationship we have with the employee, and to comply with our legal and regulatory obligations, as employer.***

## 1. WHO WE ARE

1.1 MSCL is part of the CIEL Group.

1.2 Our information details are as follows:

- **Business Registration Number**: C07002054
- **Registered office** : Georges Guibert Street, Floreal
- **Phone number**: 601-2300/605-1000

## 2. WHAT PERSONAL DATA DOES THE COMPANY COLLECT

2.1 For purposes of, and in the course of the employee's employment with the Company, we will collect or have collect the following Personal Data and information about the employee:

- **Identity Data**: First name, maiden name, last name, username, or similar identifier, marital and immigration status, title, date of birth and gender, ID card number, passport number, nationality, driving licence, immigration document such as work/residence permit or occupational permit;
- **Contact Data**: Residential address, email address, telephone including landline and mobile numbers, emergency contacts including next of kin, dependants names, addresses, and telephone number;
- **Financial Data**: Bank account details, tax account number, salary and other remuneration and benefits, national insurance number, as pensions or insurance cover;
- **Professional Data**: Details of your qualifications, skills, experience and employment history with previous employers and within MSCL Group including references;
- **Employment Records, including**:
  - details of your days of work, working hours, and attendance at work;
  - details of periods of leaves, including annual leaves, sick leaves, and other special leaves (such as maternity and paternity leaves), unpaid leaves (such as sabbaticals), reasons for any leave and any supporting documents including medical records to substantiate granting the leave;
  - details of any disciplinary or grievance procedures in which the employee has been involved, including any warnings issued to the employee and related correspondence;
  - assessments of the employee's performance, including appraisals, performance reviews and ratings, training the employee has participated in, performance improvement plans and related correspondence;
  - details of trade union membership;
  - all correspondence with the employee before, during and after your employment with the Company; and
  - Any recruitment and selection assessment report
- **Usage Data** includes information about how the employee uses the Company's computer and hardware in connection with his role and responsibilities.

2.2 **Special Categories of Data / Sensitive Data -** In some cases, the Company may require to process Sensitive Data in order to fulfill a specific purpose. Sensitive data collected are about:

- The employee's health or medical conditions including whether or not the employee has a disability for which the Company needs to make reasonable adjustments especially those employees with disabilities for complying with health and safety requirements;
- criminal records to carry out employment law obligations;
- Biometric Data to monitor attendance and to provide the employee access to the premises.

2.3 Since the above information is considered sensitive, the Processing of which may cause concern or distress to the employee, the employee's explicit Consent has been given, or will be secured, for this information to be processed if it is necessary for compliance with employment, or social protection legislation or for the purposes of personnel management and administration, suitability for employment and to comply with equal opportunity legislation.

2.4 Any Personal Data that the Company uses may be Anonymised. The employee is entirely free to decide whether or not to provide the Special Categories of Data, and there are no consequences for failing to do so except when the supply of such Special Category of Data is mandatory by law.

2.5 When providing the Personal Data of another person (next of kin, or any dependant), the employee is solely responsible for ensuring that such person is made aware of the information contained in this Privacy Notice and that the person has given his/her Consent to the employee for sharing the information with us. The employee may be required to provide data about his children, and when doing so, we shall make every reasonable effort to verify using any reasonable means (including but not limited to any written supporting evidence) that the employee's Consent as parent or guardian has been given or authorised.

2.6 If the data we collect are not listed in this Privacy Notice, we will give you (when required by law) appropriate notice of which other data will be collected and how we will be using them.

## 3. SOURCE OF PERSONAL DATA

3.1 The Company collects Personal Data about the employee in a variety of ways. The source of information is as follows:

a. Yourself directly at the start of, or during employment (such as benefit nomination forms)
b. Other CIEL Group employees
c. CIEL affiliates
d. Public authorities
e. Public websites and social media
f. Previous employers
g. Educational institutions
h. Background checks providers
i. Recruiters
j. Credit reference agencies

## 4. HOW AND WHY DOES THE COMPANY PROCESS AND CONTROL PERSONAL DATA

4.1 We will only use the employee's Personal Data when the law allows us to and in the following circumstances:

a. For the performance of the employment contract we are about to enter into or have entered into with the employee.
b. As necessary for our Legitimate Interests and the interests and fundamental rights of the employee do not override those interests.
c. Where we need to comply with a legal or regulatory obligation.

4.2 We will process the Personal Data of the employee for the purposes mentioned above based on the employee's prior Consent provided to us upon signing this Privacy Statement, and to the extent such Consent is mandatory under the Data Protection Laws.

4.3 The table below outlines all the ways we plan to control and process the Personal Data of the employee, and the legal bases upon which we rely to do so. We have also identified what our Legitimate Interests are, where appropriate. We may process Personal Data for more than one lawful ground depending on the specific purpose for which we are using the employee's data. The employee may contact us for more details about the specific legal ground(s) upon which we are relying to process Personal Data where more than one ground has been set out in the table below:

| PURPOSE | LEGAL BASIS |
|---|---|
| Managing our contractual and/or employment relationship with you. | Necessary for the performance of the employment contract to which the employee is a party. For example:<br>- to pay the employee in accordance with law and the terms and conditions of the employment contract with the Company;<br>-to administer benefits, pension, insurance entitlements or other benefits to which the employee is entitled<br>-to maintain accurate and up-to-date employment records and contact details (including details of who to contact in the event of an emergency), and records of employee contractual and statutory rights;<br>- to operate and keep a record of disciplinary and grievance processes, to ensure acceptable conduct within the workplace;<br>- to operate and keep a record of employee performance and related processes, to plan for career development, and for succession planning and workforce management purposes;<br>-to operate and keep a record of absence and absence management procedures;<br>- to provide references on request for current or former employees. |
| Recruitment and Career management | Justified on the basis of our Legitimate Interests for ensuring that we recruit the appropriate employees, we manage the promotion process, and plan for career development, and succession planning. |
| Facilitating communication with you (including in case of emergencies, and to provide you with requested information). | Justified on the basis of our Legitimate Interests for ensuring proper communication and emergency handling within the Company. |
| Operating and managing our business operations. | Justified on the basis of our Legitimate Interests for allowing effective workforce management and ensuring the proper functioning of our HR & business administration.<br>For example, it will allow us:<br>- to maintain and promote equality in the workplace; |

| | |
|---|---|
| | - to respond to and defend against legal claims. |
| Promoting the activities of the CIEL Group. | Justified on the basis of our Legitimate Interests for informing the employees of the Group of events and news concerning the business units forming part of the CIEL Group and to promote the events of the CIEL Group. |
| Complying with legal requirements | Necessary to comply with a legal and regulatory obligation to which we are subject. For example, to ensure that employees are receiving the pay or other benefits to which they are entitled.<br><br>It is also required to check an employee's entitlement to work in Mauritius, to deduct tax at source from your salary, to obtain occupational health advice comply with health and safety laws, and to enable employees to take periods of leave to which they are entitled. For certain positions, it is necessary to carry out criminal records checks to ensure that individuals are permitted to perform their duties role. |
| Monitoring your use of our IT systems (including monitoring the use of our website and any apps and tools you use). | Justified on the basis of our Legitimate Interests of avoiding non-compliance with the employment contract and protecting our reputation. |
| Performing CCTV monitoring | Justified on the basis of our Legitimate Interests inter alia to ensure the security of all employees and occupiers of the Company's premises and to protect the Company's assets and business. |
| Improving the security and functioning of our website, networks and information. | Justified on the basis of our Legitimate Interests for ensuring that you receive an excellent user experience and our networks and information are secure. |
| Making use of Biometric Data | Justified on the basis of our Legitimate Interests to monitor attendance provide the employee with access to the Company's premises. |

## 5. WHO ARE THE INTENDED RECIPIENT OF PERSONAL DATA

5.1 We routinely share the employee's Personal Data internally, including with members of the Human Resources, payroll, recruitment team, the employee's line manager, managers in the business area in which the employee works and IT staff if access to the data is necessary for performance of their duties or to monitor the Information Security Management System.

5.2 The Company may share the employee's Personal Data with Third Parties in order to obtain pre-employment references from other employers, obtain employment background checks from third-party providers or obtain necessary criminal records checks.

5.3 The Company may also share the employee's Personal Data with:

a. Its professional advisors that is accountants, auditors, lawyers, insurers, bankers, and other professional advisors within or outside of Mauritius; or
b. Any successor in title of the Company in the context of a sale, merger, acquisition, amalgamation or joint venture or otherwise any corporate or commercial action. In those circumstances the data will be subject to confidentiality arrangements.

5.4 Should the Company need to transfer employee's Personal Data to third-party recipients based outside of Mauritius, please refer to the section on '**Transfer of personal data out of Mauritius'** below.

5.5 We will share Personal Data of the employee with law enforcement or other authorities in Mauritius or elsewhere if required by applicable law, or in case of a court, administrative or governmental order to do so.

5.6 Save as herein expressly provided, we will not share Personal Data of employees with any other Third Party except with the employee's prior written Consent.

## 6. FOR HOW LONG DOES THE COMPANY KEEP PERSONAL DATA

The Company will store the employee's Personal Data for the duration of your employment or as may be required by law following termination of the employment contract.

## 7. TRANSFER OF PERSONAL DATA OUT OF MAURITIUS

7.1 We may transfer Personal Data out of Mauritius. We shall only transfer the Personal Data to another country where we hav*e* provided to the Data Protection Commissioner proof of appropriate safeguards with respect to the protection of the Personal Data and if the transfer is necessary, and we shall ensure a similar degree of security and protection is afforded to it.

7.2 Please contact us for further information. We will not otherwise transfer Personal Data outside of Mauritius.

## 8. EMPLOYEE'S RIGHTS

8.1 Under the Data Protection Laws, the employee has a number of important rights which may be exercised free of charge. In summary, those include rights to:

a) access the employee's Personal Data and obtain a copy of the data on request, which would allow the employee to check the fair Processing of information and transparency over how we use Personal Data;

b) require us to correct any mistakes in the employee's Personal Data though we may need to verify the accuracy of the new data provided to us;

c) require the erasure of Personal Data where there is no good reason for us continuing to process it.

d) ask us to delete or remove the employee's Personal Data where the employee has successfully exercised his right to object to Processing, where we may have processed the employee's Personal Data unlawfully or where we are required to erase the employee's Personal Data to comply with local laws. Note, however, that we may not always be able to comply with a request of erasure for specific legal reasons which will be notified to the employee, if applicable, at the time of request;

e) object at any time to Processing of Personal Data for Direct Marketing;

f) object to our Processing of Personal Data, where we are relying on a Legitimate Interest and there is something about the employee's particular situation which makes the employee want to object to Processing on this ground as the employee feels it impacts on his fundamental rights and freedoms. In some cases, we may demonstrate that we have compelling Legitimate Grounds to process Personal Data which override the employee's rights and freedoms;

g) request restriction of Processing of Personal Data, which allows the employee to ask that we suspend the Processing of Personal Data in the following scenarios:

(i) If the employee want us to establish the data's accuracy;

(ii) where our use of the data is unlawful but the employee does not want us to erase it;

(iii) where the employee needs us to hold the data even if we no longer require it as the employee need it to establish, exercise or defend legal claims; or

(iv) the employee has objected to our use of his data but we need to verify whether we have overriding legitimate grounds to use it.

h) lodge a complaint with the Data Protection Commissioner. In this case, we would appreciate the chance to deal with the employee's concerns before approaching the Data Protection Commissioner, so please contact us in the first instance.

i) withdraw his Consent, at any time, where we are relying on such Consent to process the employee's Personal Data. However, this will not affect the lawfulness of any Processing carried out before the employee withdraws his Consent. If the employee withdraws his Consent, we may not be able to manage our relationship with him or comply with our legal and regulatory obligations. We will advise the employee if this is the case at the time he withdraws Consent.

8.2 If the employee would like to exercise any of the above rights, please:

a) write to us as set out under the section '**How to Contact Us'** below.

b) let us have enough information to identify the employee,

c) let us have proof of the employee's identity and address (a copy of the employee's driving licence or passport and a recent utility or credit card bill), and

d) let us know the information to which the request relates.

8.3 If the employee would like to unsubscribe from any *email newsletter* or other means of Direct Marketing the employee can also click on the 'unsubscribe' button at the bottom of the *email newsletter* or exercise his option to opt out from receiving marketing materials from us.

## 9. HOW DO WE PROTECT PERSONAL DATA

9.1 The Company takes the security of Personal Data seriously. Personal Data is stored in a range of different places, including in the employee's personnel file, in the organisation's HR management systems and in other IT systems (including the organisation's email system).

9.2 We have appropriate security and organisational measures in place to prevent Personal Data from being accidentally lost, or used or accessed in an unauthorised way, and ensure compliance with our legal and regulatory obligations under the Data Protection laws. These measures are fully set out in MSCL Data Privacy Policy to which the Company fully adheres.

9.3 We limit access to the employee's Personal Data to those who have a genuine business need to know it. Those Processing your Personal Data will do so only in an authorised manner and are subject to a duty of confidentiality.

9.4 We also have procedures in place to deal with any suspected data security breach. We will notify the employee and the Data Protection Commissioner of any suspected data security breach.

## 10. CHANGES TO THIS PRIVACY NOTICE

10.1 This Privacy Statement was published on 15th February 2019

10.2 We may change this Privacy Statement from time to time, when we do we will inform the employee via email .

## 11. HOW TO CONTACT US

11.1 Please contact us by writing to the Data Protection Officer as follows:

Data Protection Officer
MSCL
c/o Jenna Li Ying
Telephone: 6012300

Email: jenna.li@cliniquedarne.com

**12. EMPLOYEE'S EXPRESS CONSENT – PLEASE READ CAREFULLY**

***"By signing and returning a duplicate of this notice, I hereby Consent that the Company processes my Personal Data, as described in this Privacy Notice, and undertake to immediately notify the Company, in the event I have any question, or wish to exercise any of my rights as described herein."***

**Employee Signature** _____

**Employee Name** _____

**Date** _____

# Appendix F: Template of End User Notice

This computer system (including all hardware, software and peripheral equipment) is the property of MSCL. It should strictly only be used for business purposes and should not be used to store the personal data of the user. All users should ensure that the use of the computer system is at all times compliant with MSCL IT Security Policy and protocols and MSCL reserves the right to monitor the use of the computer system to ensure its compliance with its security protocols. Any additional monitoring, such as monitoring of performance or working hours, shall only take place if permitted in accordance with local laws, regulations and/ or policies. Any unauthorised access, use or modification of the computer system may be sanctioned in accordance with local laws, regulations and/ or policies.

# Appendix G: Template of privacy breach register

| Breach Reference | Details of breach | | | | | | | | | | | Measures Taken | | Severity | Action plan | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Date of breach occurrence (or approximation) | Date of breach identification | How [name of business unit] became aware of breach? | Location of the breach | Breach at third party? (if yes, identify which third party) | Type of breach | Description of breach | Suspected cause of breach | Description of PII affected (nature and content) | Type of data subjects affected | No. individuals affected (or approximation) | Measures taken to prevent breach | Measures operated effectively? | Breach severity (following assessment) | Remedial action | Supervisory Authority informed? | Date of notification | Data subjects informed? | Date of notification |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | |

# Appendix H: Privacy breach severity assessment methodology

The following scales must be used by business units across all clusters for assessing the severity of privacy breaches.

- Rating scale for type of data

This parameter identifies the type of data affected by the privacy breach to assign a rating based on the following criteria:

| Score | Description |
|---|---|
| 1 | Non-sensitive categories of personal information (such as name, location, email addresses etc.) |
| 2 | Non-sensitive categories of personal information that can be used to extrapolate the profile of the affected data subjects (such as information permitting the assumption of a person's financial status) |
| 3 | Special categories of personal information (such as medical records, religious beliefs, sexual orientation, criminal records etc.) |

- Rating scale for ease of identification

This parameter identifies the ease with which a data subject's identity can be determined by an unauthorised party based on the data that has been breached. A rating is assigned based on the following criteria:

| Score | Description |
|---|---|
| 1 | Data is anonymised, encrypted or has been rendered illegible to an unauthorised party |
| 2 | Data is in plain text and permits the identification of a data subject by an unauthorised party |

- Rating scale for receiver of the breach

This parameter defines the parties with access to the breached information and their potential intent. A rating is assigned based on the following criteria:

| Score | Description |
|---|---|
| 1 | Breach permits known receivers to have access to the personal information (for example, email is sent to the wrong addressee) |
| 2 | Breach permits known receivers with potential malicious intent to access the data (for example excessive access rights may be granted to disgruntled employees) |
| 3 | Breach permits unknown receivers to have access to the personal information (for example hackers) |

- Method for assessing severity of the privacy breach

The severity privacy breach is assessed by combining the three-above mentioned criteria to obtain an overall severity rating which is then analysed in line with the scale below.

Severity rating = score for type of data + score for ease of identification + score for receiver of breach information.

| Rating | Description |
|---|---|
| 4 or less | Breach is not likely to result in a risk as data subjects either will not be affected or minor inconveniences (for example need to change password, re-confirm information etc.) may result. MSCL should document the breach in their breach register and monitor until closure. |

| Rating | Description |
|---|---|
| 5 to 6 | Breach is likely to result in a risk and data subjects may encounter inconveniences which may prove to be difficult to overcome (for example, fear, costs, inability to access their personal information, etc.). MSCL should inform the Supervisory Authority of the breach and document the breach in the breach register. |
| 6 or more | Breach is likely to result in a high risk to the data subjects and the latter may encounter significant and irreversible damage (for example, misappropriation of funds, psychological or physical distress, loss of employment, death etc.). MSCL should inform the Supervisory Authority as well as the affected data subjects and document the breach in the breach register. |

# Appendix I - Guidelines on the use of CCTV and recording of CCTV data.

## Example of notice

These premises are under CCTV surveillance. This CCTV system and the images produced by it are controlled by (to be defined by each business unit), who is responsible for how the system is used. (Name of business unit) has considered the need for using CCTV and has decided it is required for the prevention and detection of crime and for protecting the safety of its employees and customers. It will not be used for other purposes. We conduct an annual review of our use of CCTV.

## Guidelines on the use of CCTV

- There is a named individual for each business unit who is responsible for the operation of the system.
- Access controls to the CCTV and recordings are in place and are defined by each business unit. Decisions to share CCTV recordings with third parties (such as law enforcement bodies) are approved by senior management of each business unit and documentation of approval is retained. A list of third parties which whom CCTV recordings can be shared is established and documented.
- The problem the business unit is trying to address by installing cameras is clearly defined and decision that installation of cameras is identified as the best solution is documented. This decision is reviewed on a regular basis.
- A system which produces clear images and which the law enforcement bodies (usually the police) can use to investigate crime is chosen. Images can easily be taken from the system when required.
- Cameras are positioned so that they provide clear images.
- Cameras are positioned to avoid capturing the images of persons not visiting the premises.
- There are visible signs showing that CCTV is in operation.
- Images from the CCTV system are securely stored, where only a limited number of authorised persons have access to them. Level of access of the service provider is also determined.
- The recorded images are retained long enough for any incident to come to light (e.g. for a theft to be noticed) and the incident to be investigated. Timeframes for retention of recordings are clearly defined.
- The potential impact on individuals' privacy is identified and taken into account in the use of the system.
- The business unit implements measures to respond to individuals making requests for copies of their own images.
- Regular checks are carried out to ensure that the system is working properly and is producing high quality images. These checks are documented.

# Appendix J - Fingerprinting Consent Form

I, [Name of Employee], consent to the collection of my fingerprints by my Employer for purposes of [recording attendances/ access control during/outside working hours].

I acknowledge and understand that my fingerprints will be processed and retained by my Employer solely for the purposes specified above in accordance with its Data Privacy Policy and in strict compliance with the provisions of the Data Protection Act 2017, the EU General Data Protection Regulations, where applicable, or any other applicable legislation.

I understand that I may, at any time, without the need to justify my decision, object to fingerprinting without this impacting, in any way, my contract of employment with my Employer.

Name of Employee _____

Signature of Employee _____

Date _____