


<b>Identifier:</b>	Version:	Effective Date:	 The Medical and Surgical Centre Limited
MSCL-COM POL-002	V0	15/02/2019	
Original Date: <b>YYYY/MM/DD</b>	31/01/2019		
Document Owner:	<u>MANAGER- BUSINESS ANALYTICS</u>		

## MSCL – Compliance

# PERSONAL DATA BREACH 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
<i>Head of HR</i>	<i>28/01/2019</i>		<i>Clive Chung</i>
<i>Chief Operating Officer</i>	<i>31/01/2019</i>		<i>Claire Wanquet/Olivier Schmitt</i>

---

### Document Approval

This document requires following approvals:

Title	Date	Signature	Name
<i>Chief Executive Officer</i>	<i>31/09/2019</i>		<i>Olivier Schmitt</i>

PLEASE MAKE SURE THAT THIS IS THE CURRENT VERSION BEFORE USE.  
ONCE PRINTED, THIS IS AN UNCONTROLLED DOCUMENT.

This document is proprietary, confidential and intended only for the internal use of recipients. No part of this document may be disclosed in any manner to a third party without the prior written consent of MSCL.

**Confidential**  
For Internal Use Only

<b>Purpose</b>	This policy defines requirements when a data breach happens in the organisation
<b>Scope</b>	This policy is for employees to understand and report the process in case of personal data breach
<b>Responsibility</b>	MSCL Data Protection officer
<b>Definitions</b>	Refer to section 5 glossary (pg18)
<b>Links to other Policies/Documents</b>	Personal Data Breach Policy
<b>References</b>	<a href="http://dataprotection.govmu.org">http://dataprotection.govmu.org</a> <a href="https://eugdpr.org/">https://eugdpr.org/</a>
<b>Training</b>	All MSCL employees
<b>Distribution</b>	All MSCL employees

## Contents

1. Introduction .....	4
1.1. Purpose .....	4
1.2. Objective .....	4
2. Personal Data Breach.....	4
3. Breach Identification, Investigation, Notification and Reporting Line.....	5
4. Information to be included in the Breach Notification Form to the Supervisory Authority .....	7
5. Notification outside of the 72 hours.....	8
6. Notification to individuals affected by the Personal Data Breach .....	8
7. Breach Register .....	9
8. Other reporting obligations .....	9
9. Improving organisational measures to prevent future breaches .....	9
10. Confidentiality.....	9
11. Sanctions for breaching this Personal Data Breach Policy.....	9
12. Glossary.....	10
Schedule 1 - Privacy breach severity assessment methodology .....	10
Schedule 2 – Breach Notification Form prescribed by the Data Protection Commission .....	13
Schedule 3 –Breach Register template .....	15
Schedule 4 – List of EU National Supervisory Authorities .....	16

## 1. Introduction

### 1.1. Purpose

A Personal Data Breach may, if not addressed in an appropriate and timely manner, result in substantial damage to individuals affected by the breach such as loss of control over their Personal Data, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of Personal Data protected by professional secrecy or any other significant economic or social disadvantage. Swift containment and recovery from a Personal Data Breach is therefore vital.

The Data Protection Act 2017 (“DPA”) (which applies to the processing of the Personal Data of Data Subjects in Mauritius) and the EU General Data Protection Regulation (“GDPR”) (which applies to Controllers in the European Union but also in some cases, to Controllers outside the European Union but processing Personal Data of Data Subjects who are in the European Union) (together referred to as “the Data Protection Laws”) impose a duty on all Controllers to notify the Supervisory Authority of a Personal Data Breach without undue delay and, where feasible, **not later than 72 hours after having become aware of it**. Subject to a few exceptions, the Data Protection Laws also impose a duty on all Controllers to communicate a Personal Data Breach to the Data Subject without undue delay where a Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subject concerned by the breach.

This Personal Data Breach Policy (“Data Breach Policy”) is related to the MSCL Data Privacy Policy dated 15<sup>th</sup> February 2019 (“Data Privacy Policy”). It further defines the policy of MSCL to ensure that all of its business units and employees maintain the privacy of personal information held in physical files or in electronic form by implementing appropriate organisational measures to detect, manage, escalate, respond to and report a Personal Data Breach as and when it arises with a view to promoting a data privacy culture within MSCL and in compliance with the Data Protection Laws.

### 1.2. Objective

The Objective of this Data Breach Policy is for MSCL to develop a robust breach reporting process in order to comply with the Data Protection Laws. In particular, this Data Breach Policy defines:

1. what amounts to a Personal Data Breach;
2. the breach management, notification and escalation process;
3. the methodology for assessing the severity of a Personal Data Breach;
4. information to be included in a breach notification to the Supervisory Authority;
5. information to be included in a breach notification to a Data Subject, where there is a duty to notify;
6. additional notification obligations in the event of a Personal Data Breach;
7. information to be included in the Breach Register to be maintained by each business unit for communication to the Supervisory Authority / Data Subjects upon requests;
8. confidentiality obligations when managing a Personal Data Breach; and
9. sanctions for failing to comply with this policy.

## 2. Personal Data Breach

A Personal Data Breach is defined under the Data Protection Laws to mean a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to,

Personal Data transmitted, stored or otherwise processed by the Controller or a Processor. This includes breaches that are the result of both accidental and deliberate causes. For purposes of the Data Protection Laws, Personal Data is any information relating to a living identified or identifiable individual.

Examples of Personal Data Breaches include:

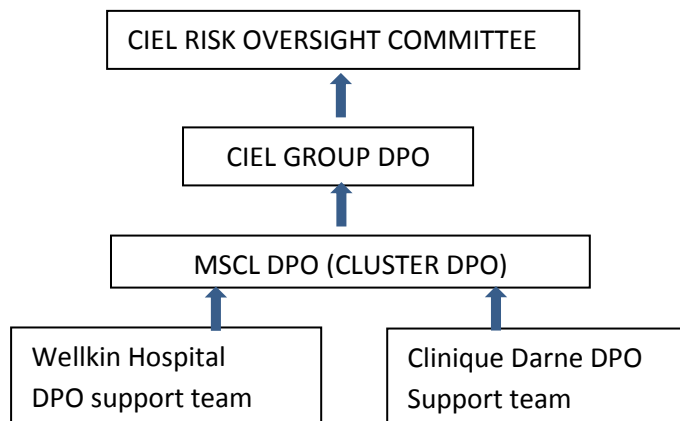
1. sending Personal Data (accidentally or deliberately) to internal or external persons who do not have a legitimate need to have access to such Personal Data;
2. databases containing Personal Data being compromised, for instance by being illegally accessed by hackers;
3. an intruder stealing or accessing a device containing a Controller's customer database and misusing it to impersonate the customers.
4. loss or theft of computer devices, mobile devices, or paper records containing Personal Data;
5. paper records containing Personal Data being left unprotected for anyone to see;
6. staff accessing or disclosing Personal Data outside the requirements or authorisation of their job;
7. being deceived by a third party into improperly releasing the Personal Data of another person; and
8. the loss of Personal Data due to unforeseen circumstances such as a fire or flood.

Where a Processor becomes aware of a Personal Data Breach, he shall notify the Controller without any undue delay.

### **3. Breach Identification, Investigation, Notification and Reporting Line**

Under the Data Protection Laws, all Personal Data Breaches must be reported to the Supervisory Authority **within 72 hours** of the Controller becoming aware of the said breach. Failing to do so without good and justifiable reasons would amount to a breach of the DPA rendering the Controller liable to a fine of up to Rs200,000 and to imprisonment for term not exceeding 5 years (where the Personal Data Breach falls under the DPA) or to a fine of up to EURO 20 million or up to 4% of MSCL annual turnover (where the Personal Data Breach falls under the GDPR). In addition, under the GDPR, the fine may be combined with other regulatory sanctions including an order for the forfeiture of any equipment or any article used or connected in any way with the commission of an offence.

The following structure summarises the steps to be taken to escalate a Personal Data Breach as soon as the Controller becomes aware of the said breach.



All identified, actual or possible, Personal Data Breaches must immediately be reported by the employee discovering the breach to the DPO of MSCL or to the DPO Support team at the hospital where the breach occurred. If the breach is IT related, the IT officer of the business unit must also be immediately notified by the employee in order for the latter to take immediate actions to contain the risks.

The MSCL DPO must thereafter immediately start a preliminary investigation to determine the nature and severity of the Personal Data Breach including:

1. when the breach occurred;
2. suspected cause (s) of the breach;
3. description of the Personal Data Breach including the nature and content of the Personal Data Breach;
4. categories and number of living individuals affected by the breach;
5. in the case of communication of the Personal Data breach to Data Subjects, the likely consequences of the breach and whether the breach is likely to result in a high risk to the rights and freedoms of the persons affected by the breach. The severity of the breach is to be assessed based on the methodology set out under **Schedule 1** to this Personal Data Breach Policy.
6. The measures taken to contain the risks associated with the breach or proposed to be taken to deal with the breach.

Once the relevant information has been gathered, the MSCL DPO should immediately inform the Group DPO of the Personal Data Breach and provide a report to the latter on the investigation conducted.

The MSCL DPO, following consultation with the Group DPO (where feasible), should without undue delay and, where feasible, **not later than 72 hours after having become aware of the Personal Data Breach** inform the Supervisory Authority of the Personal Data Breach.

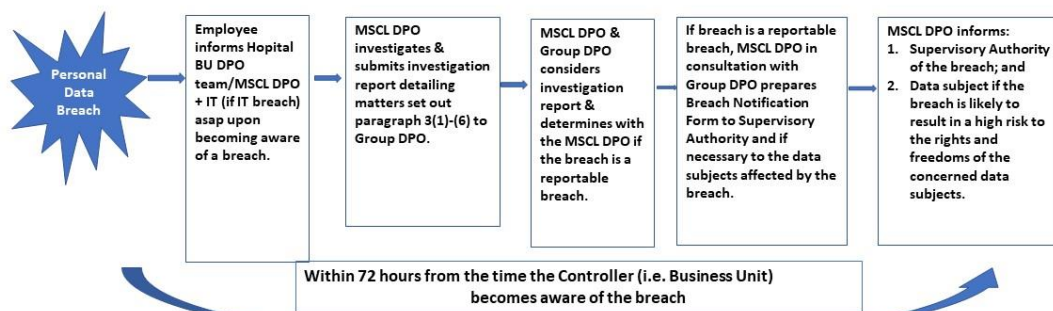
The MSCL DPO, following consultation with the Group DPO (where feasible), should communicate a Personal Data Breach to the Data Subject without undue delay where the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Data Subject, unless the exceptions, as provided by the Data Protection Laws, apply.

For all breaches arising out of data processed in Mauritius, the MSCL DPO must notify the Data Protection Commissioner in Mauritius by completing the prescribed “**Personal Data Breach Notification Form**” set out under **Schedule 2** to this Personal Data Breach Policy (available on the website of the Data Protection Office at <http://dataprotection.govmu.org>) and sending it to the Data Protection Commissioner at the following address (for all breaches taking place in Mauritius):

The Data Protection Commissioner,  
 Data Protection Office,  
 5th Floor, SICOM Tower  
 Wall Street, Ebène

For all breaches where the GDPR applies, the MSCL DPO must, following consultation with the Group DPO, notify the relevant Supervisory Authority of the European Union member where the Personal Data Breach has occurred as listed under **Schedule 4** of the breach. Where the Controller has appointed an EU Representative, notification to the relevant Supervisory Authority shall be carried out through the EU Representative.

The following flow-charts summarise the steps to be followed when a Personal Data Breach occurs:



- Notes:
1. If the breach is reported after 72 hours, reasons for the delay must be provided to the Supervisory Authority .
  2. Depending on the severity of the breach as unveiled by the investigation report, the MSCL DPO in consultation with the Group DPO may determine not to inform the data subject of the breach, if a statutory exemption applies.
  3. Other than the Supervisory Authority, the MSCL DPO may need to notify other regulatory authorities and third parties of the breach such as the police, the FIU, banks, the Bank of Mauritius, the Financial Services Commission and insurance companies.

#### 4. Information to be included in the Breach Notification Form to the Supervisory Authority

The Data Protection Commission has published a prescribed form for Controllers to use when notifying a Personal Data Breach to the Data Protection Commissioner in Mauritius for breaches arising out of Personal Data processed in Mauritius (i.e breaches falling under the scope of the DPA). A copy of the “**Personal Data Breach Notification Form**” is set out under **Schedule 2** to this Personal Data Breach Policy.

For all other breaches falling under the scope of the GDPR (eg. concerning the processing of the Personal Data of people in the European Union), the following information must be provided to the Supervisory Authority listed under **Schedule 4** (either directly or through the services of the EU Representative):

1. a description of the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
2. a description of the likely consequences of the Personal Data Breach;
3. a description of the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

#### **5. Notification outside of the 72 hours**

Where the Controller cannot meet the delay of 72 hours to report a Personal Data Breach to the Supervisory Authority, the Controller must provide reasons for the delay. Under the GDPR, where the Controller has not been able to complete its investigation within 72 hours or where it is not possible to provide the full information at the same time, the information may be provided to the Supervisory Authority in phases without further undue delay.

#### **6. Notification to individuals affected by the Personal Data Breach**

When the Personal Data Breach is likely to result in a high risk to the rights and freedoms of individuals, the Controller must also communicate the Personal Data Breach to the Data Subject without undue delay. The severity of the breach is to be assessed based on the methodology set out under **Schedule 1** to this Personal Data Breach Policy. The notification must contain the following information in clear language:

1. a description of the nature of the Personal Data Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;
2. a description of the likely consequences of the Personal Data Breach;
3. a description of the measures taken or proposed to be taken by the Controller to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. the name and contact details of the Data Protection Officer or other contact point where more information can be obtained;

The Controller is not required to notify the Data Subjects of the Personal Data Breach where the Controller can show that:

1. it has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal Data affected by the Personal Data Breach, in particular, those that render the Personal Data unintelligible to any person who is not authorised to access it, such as encryption;
2. it has taken subsequent measures which ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialise; or
3. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.



Where the controller has not already communicated the Personal Data Breach to the Data Subject, the Commissioner may, after having considered the likelihood of the personal data breach resulting in a high risk, require it to do so.

## **7. Breach Register**

The Controller must under the Data Protection Laws document the facts relating to a Personal Data Breach, the effects thereof and the remedial action taken by the Controller.

Accordingly, all business units must maintain a Breach Register of all Personal Data Breaches, whether or not such breaches have been reported to the Supervisory Authority. A template of a Breach Register is set out under **Schedule 3** to this Personal Data Breach Policy.

## **8. Other reporting obligations**

Depending on the nature of the Personal Data Breach, there may be additional notification obligations under other laws to be considered including notifying third parties such as the police, insurers, professional bodies, banks, Financial Intelligence Unit, credit card companies or other regulatory bodies who can help to reduce the risks of financial loss to individuals. Each case must be assessed on its own merits.

## **9. Improving organisational measures to prevent future breaches**

As with any security incident, the business units affected by the Personal Data Breach should investigate whether or not the breach was as a result of human error or a systemic issue and be proactive and innovative to implement preventative measures to guard against future risks of a similar nature occurring – including training its staff, having robust contracts with appropriate warranties from third party processors, implementing appropriate processes to detect Personal Data Breach at an early stage and to contain the associated risks, consider encryption/pseudonymisation of data, amongst other measures designed to protect the Personal Data of individuals controlled by the relevant business unit.

## **10. Confidentiality**

The management of a Personal Data Breach and any document prepared or furnished in connection therewith shall be kept strictly confidential by all members of the data protection team working on the breach. Information concerning the Personal Data Breach must be communicated only to those on a strictly needs-to-know basis.

## **11. Sanctions for breaching this Personal Data Breach Policy**

A breach of this Personal Data Breach Policy by an employee amounts to a breach of the latter's employment agreement and may result in disciplinary actions being taken against the said employee by the relevant business unit concerned by the breach.

## 12. Glossary

- Breach Register:** means the register set out under **Schedule 3** which should be used and maintained by all business units across clusters to record a breach incident.
- Controller:** means a person which, alone or jointly with others, determines the purposes and means of the processing of Personal Data and which has decision making power with respect to the processing;
- Data Subject:** means an identified or identifiable individual, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;
- Personal Data:** any information relating to a Data Subject;
- Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;
- Processor:** means a person who, or public body which, processes personal data on behalf of a Controller;
- Data Protection Laws:** For purposes of this Personal Data Breach Policy, Data Protection Laws mean collectively the General Data Protection Regulations (EU Regulation 2016/679) and the Data Protection Act 2017; and
- Special categories of Personal Data** means personal data pertaining to a person's:
- (a) racial or ethnic origin;
  - (b) political opinion or adherence;
  - (c) religious or philosophical beliefs;
  - (d) membership of a trade union;
  - (e) physical or mental health or condition;
  - (f) sexual orientation, practices or preferences;
  - (g) genetic data or biometric data uniquely identifying him;
  - (h) the commission or alleged commission of an offence by him; or
  - (i) any proceedings for an offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any Court in the proceedings.
- Supervisory Authority:** The Supervisory Authority in Mauritius is the Data Protection Commissioner. Where the GDPR applies, the relevant Supervisory Authority would be as per the list set out under **Schedule 4** below.

### Schedule 1 - 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.) (More fully defined in the Glossary)

- 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. The Controller should document the breach in their Breach Register and monitor until closure. The Controller should notify the Data Protection Commissioner of the breach. If the breach falls under the GDPR, the Controller should determine whether to notify the Supervisory Authority depending on the nature of the risk. Depending on the specific circumstances of the Personal Data Breach, the Controller should assess on whether to notify to the Data Subject of the breach.
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.). The Controller should notify the Supervisory Authority

Rating	Description
	of the breach and communicate the breach to the Data Subject (unless exceptions apply) 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, etc.). The Controller should inform the Supervisory Authority of the breach and communicate the breach to the Data Subject (unless exceptions apply) and document the breach in the Breach Register.

## Schedule 2 – Breach Notification Form prescribed by the Data Protection Commission

### Personal Data Breach Notification

Under section 25 of the Data Protection Act, in case of a personal data breach<sup>1</sup>, the controller<sup>2</sup> shall without undue delay and where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Data Protection Office.

Swift containment and recovery from a personal data breach is vital. Every effort should be taken to minimise the potential impact on affected individuals, and details of the steps taken to achieve this should be included in this form. If you are waiting for completion of an internal investigation, please tell us.

#### 1. Particulars of controller giving the notification

(a) Name of controller: \_\_\_\_\_

(b) Address: \_\_\_\_\_

(c) Is the controller registered with the Data Protection Office(Y/N)? \_\_\_\_\_

(d) Name of processor<sup>3</sup> where the data breach occurred (if applicable):

\_\_\_\_\_

(e) Telephone number of controller: \_\_\_\_\_ Fax number: \_\_\_\_\_

(f) Email address of controller \_\_\_\_\_

(g) Name of Designated Data Protection Officer (\*Mr./Ms./Mrs):

\_\_\_\_\_

#### (\*Please delete as appropriate)

(h) Designation: \_\_\_\_\_

(i) Telephone number: \_\_\_\_\_

\_\_\_\_\_

(j) Email address: \_\_\_\_\_

**2. Nature of the personal data breach**

(a) When did the personal data breach happen?

---

(b) If there has been a delay (more than 72 after becoming aware of the incident and reporting it to the Data Protection Office), please provide your justifications for the delay:

---

---

(c) Describe the personal data breach in as much detail as possible including cause(s)

---

---

---

---

---

---

---

---

### Schedule 3 –Breach Register template

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 Personal Data 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

**Schedule 4 – List of EU National Supervisory Authorities**

(updated on 19 April 2018, accessible at [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612080](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080))