Privacy Policy

Protection of Personal Information, Information Security and Records Management Policy for

Mobile Therapy (CC) t/a MJ Labs

Registration Number: 1999/014221/23

(Hereinafter referred to as "**the Collecting Party**")

Collection of Personal Information in terms of the Protection of Personal Information Act 4 of 2013.

Version Number:	*1*
Date:	2023/09/20
Superseded by:	N.A
Information Officer (Signature):	

Contents

Collection of Personal Information in terms of the Protection of Personal Information Act 4 of 2013. 1
1. Introduction 3
2. Background 3
2.1 **What is the Purpose of the Act** 3
2.5 How is 'Personal Information' defined? 4
2.8 **What does the Processing of Personal Information entail?** 4
2.9 **Who is compelled to comply?** 4
2.10 **What does compliance entail?** 5
2.11 **Limitation of Processing** 5
2.11.4 **Purpose specification** 6
2.11.6 **Use limitation** 6
2.11.7 **Information Quality** 6
2.11.8 **Transparency (Openness)** 6
2.11.9 **Security Safeguards** 6
2.11.10 **Data Subject Participation** 7
2.12 **Compliance Guides** 7
2.13 **Details of Information Officer(s)** 7
3. Personal Information Collected 8
4 **The use of Personal Information** 9
5 **Disclosure of Personal Information** 9
6. **Safeguarding Personal Information** 10
7. **Correction of Personal Information** 10
8. **Amendments to this Policy** 11
9. **Access to Documents** 11
10. **Requests for the Collector's Information** 11
11. **Retention of Documents** 11
12. **Destruction of Documents** 12
13. **Cross-Border Flow of Information** 12

1. Introduction

1.1 The Collecting Party is an Industry Specific Contract Manufacturer and Fortifier for Complementary Medicine, and Food stuff in the Commercial-, wholesale-, e-commerce and related -sectors. The Collecting Party maintains a website in order to better connect with prospective clients and as a result handles Personal Information, which is submitted to the end of forming prospective business relationships with the public. This handling of personal information mandates the collecting party to comply with the *Protection of Personal Information* Act 4 of 2013.[1]

1.2 The Act mandates that the Collecting Party inform their clients in the way personal information is used, altered, disclosed and destroyed. The collecting party is committed to its mandate in terms of all national- or otherwise, that which is law, to handle collected Personal Information with care and confirming that such information is used transparently, securely and appropriately.

1.3 This policy sets out how the collecting party gathers and treats Personal Information and to what purpose and extent such information is used.

1.4 This policy is available at the registered physical address of the collecting party, as well as electronically on the website of the collecting party.

2. Background

2.1 **What is the Purpose of the Act**

2.2 The aim of the Act is to ensure the right of South African citizens to the privacy of personal information and to regulate all organisations that collect, store and disseminate personal information.

2.3 Personal Information Processing may only take place if it complies with the framework provided for by the Act.

2.4 Processing of Personal Information may only take place in accordance with the following prescribed and defined conditions:

2.4.1 Accountability
2.4.2 Limitations of Processing
2.4.3 Specification of Purpose
2.4.4 Limitations of Use
2.4.5 Information Quality
2.4.6 Transparency (Openness)
2.4.7 Security Safeguards
2.4.8 Individual (Data Subject) Participation

[1] Hereafter referred to as "the Act".

2.5 How is 'Personal Information' defined?

2.6 Personal information means any information relating to an identifiable natural person (and existing juristic persons where applicable), including information relating to:

2.6.1 race, gender, sex, pregnancy, marital status, mental health, well-being, disability, religion, belief, culture, language, and birth.

2.6.2 education, medical, financial, criminal or employment;

2.6.3 identity number(s), electronic and physical addresses, telephone numbers and on-line identifiers;

2.6.4 biometric information;

2.6.5 personal opinions, views or preferences;

2.6.6 correspondence sent by a person implicitly or explicitly of a personal nature or confidential.

2.7 The collecting party may not process personal information of a child (under the age of 18) unless:

2.7.1 the processing is carried out with the consent of the legal guardian.

2.7.2 the processing is necessary to establish, exercise or in defense of a right or obligation in law;

2.7.3 the processing is necessary for historical, statistical or research purposes; or

2.7.4 the processing is information that is deliberately made public by the child with the consent of the guardian.

2.8 **What does the Processing of Personal Information entail?**

2.8.1 Processing means any operation or activity, or set of activities, by automatic means or otherwise, including:

2.8.2 collecting, receiving, recording, collating, storing, updating, modifying, retrieving or use;

2.8.3 disseminating by means of transmission, distribution or any other means; or;

2.8.4 merging, linking, restricting, erasing or destroying information.

2.9 **Who is compelled to comply?**

2.9.1 All persons, natural or juristic; public or private, must comply.

2.10 **What does compliance entail?**

2.10.1 Accountability

2.10.1.1 Organisations must assign responsibility to ensure compliance with the Act to a suitable person or persons.

2.10.1.2 Each organisation has an "information officer". This will be the same person who has been appointed by the organisation as head in terms of the Promotion of Access to Information Act.

2.10.1.3 The information officer, together with an executive team/board, should decide on and record the POPI policy and procedure (this policy).

2.10.1.4 The information officer must appoint a '*data controller*' or several data controllers who decide:

2.10.1.4.1 the purpose of the data processing; and

2.10.1.4.2 the way personal information should be processed.

2.10.1.5 The data controllers should be the management who execute the POPI policy and procedure.

2.10.1.6 '*Data processor(s)*' perform the processing administration.

2.11 **Limitation of Processing**

2.11.1.1 Personal information may only be processed if it is:
2.11.1.2 adequate, relevant and necessary for the purpose for which it is processed;
2.11.1.3 with the consent of the data subject
2.11.1.4 necessary for the contract to which the data subject is party;
2.11.1.5 necessary for the protection of a legitimate interest of the data subject;
2.11.1.6 required by law;
2.11.1.7 necessary to pursue the legitimate interest of the collector; or
2.11.1.8 collected directly from the data subject.

2.11.2 "Consent" must be:

2.11.2.1 voluntary;
2.11.2.2 specific; and
2.11.2.3 informed.

2.11.3 Informed consent requires that the data subject understand:

2.11.3.1 what information is being collected/processed;
2.11.3.2 why the information is being processed;
2.11.3.3 how the information is to be processed;
2.11.3.4 where the information is being processed; and
2.11.3.5 to whom the information is intended to be given.

2.11.4 **Purpose specification**

2.11.5 The data subject must be made aware of the purpose for which the information is being collected (such as the “identified purpose”). This is necessary for giving consent (see above).

2.11.6 **Use limitation**

2.11.6.1 Information/records may only be kept for as long as it is necessary to achieve the identified purpose. There are some statutory records keeping periods which may exceed this period.

2.11.6.2 After this retention period the responsible person must delete or destroy such information as soon as reasonably possible.

2.11.6.3 If the purpose changes (e.g., something else occurs that could use the same information again for this alternative purpose), it may be necessary to inform the data subject and get consent again.

2.11.7 **Information Quality**

2.11.7.1 Information must be as accurate as possible, complete and updated if necessary.

2.11.7.2 Information must be available to the data subject to verify/object to the accuracy thereof.

2.11.8 **Transparency (Openness)**

2.11.8.1 The Collector must take reasonable practical steps to ensure that the data subject is aware of what personal information is being collected, stored and used, and/or collected directly from the data subject.

2.11.9 **Security Safeguards**

2.11.9.1 The Collector must secure the integrity and confidentiality of personal information and must take appropriate technical / organisational measure to prevent:

2.11.9.1.1 the loss of or damage to personal information; or

2.11.9.1.2 the unlawful access to or processing of personal information.

2.11.9.2 To do this, the Collector must:

2.11.9.2.1 identify all reasonably foreseeable internal and external risks to personal information held;

2.11.9.2.2 establish and maintain appropriate reasonable safeguards against the risks;

2.11.9.2.3 monitor the safeguards and regularly verify safeguards are effective; and

2.11.9.2.4 ensure safeguards are updated to respond to new risks or deficiencies in previous safeguards.

2.11.9.3 The data controllers and data processors must operate under his/her authority from the information officer and treat all personal information as confidential.

2.11.9.4 Where there are reasonable grounds for suspecting a breach of data security, the responsible person must notify the Regulator and the data subject.

2.11.10 **Data Subject Participation**

2.11.10.1 Any person who can positively identify themselves is entitled to access their own personal information.

2.11.10.2 A data subject has the right to correct or amend any of their personal information that may be inaccurate, misleading or out of date.

2.12 **Compliance Guides**

2.12.1 An audit should be conducted of the following:

2.12.1.1 what personal information is held?
2.12.1.2 where the personal information is being held?
2.12.1.3 by whom is the personal information being held?

2.12.2 Establish what personal information is being collected in one place and being transferred to another.

2.12.3 Review privacy statements, email indemnity, supplier or other standard terms and conditions, engagement letters, employee letters of appointment and third-party agreements that will process personal information of your clients or customers.

2.12.4 Develop organisation wide standard data protection policies and protocols, and if in place already in place, review such policies and protocols.

2.12.5 Review IT outsourcing contracts and arrangements.

2.12.6 Review data collecting activities (completion of forms etc).

2.12.7 Appoint an information officer for POPI and PAIA purposes.

2.12.8 Provide training to staff.

2.13 **Details of Information Officer(s)**

2.13.1 The details of the Collector's Information Officers are as follows:

INFORMATION OFFICER	Ruan Steyn
EMAIL ADDRESS	ruan@mjlabs.co.za
DEPUTY INFORMATION OFFICER	Sharne' Combrink
EMAIL ADDRESS	validation@mjlab.co.za

DEPUTY INFORMATION OFFICER	Bethe Seyffert
EMAIL ADDRESS	rnd@mjlabs.co.za
DEPUTY INFORMATION OFFICER	Luka Cadle
EMAIL ADDRESS	luka@mjlabs.co.za
DEPUTY INFORMATION OFFICER	Michaela Skinner
EMAIL ADDRESS	ft@mjlabs.co.za
BUSINESS ADDRESS	354 Derdepoort Road, Silverton, 0044.
TELEPHONE NUMBER	012 804 8966

3. Personal Information Collected

3.1 Section 9 of the Act provides that information may only be collected on the basis that such information collection is, through the scope of the purpose for which it is collected, adequate, relevant and not excessive.

3.2 The Collector gathers Personal Information solely for the following reasons:

3.2.1 to provide manufacturing and technical services to clients interested in complementary medicine.

3.2.2 to provide development, formulation and all ancillary services to clients interested in complementary medicine formulation.

3.2.3 to assist with product label contents, design and printing.

3.2.4 to conduct customer satisfaction reviews.

3.2.5 internal Human Resource purposes.

3.2.6 through cookies and related technologies to record information about a client's device, its browser, and, in some cases, its preferences and browsing habits; and

3.2.7 in connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law.

3.3 The type of information will depend on the need for which it is collected and will be processed for that purpose only.

3.4 Whenever possible, the Collector will inform the client as to the information required and the information deemed optional.

3.5 The Collector processes the client's personal information for marketing purposes in order to ensure that our products and services remain relevant to our clients and potential clients.

3.6 The Collector aims to have agreements in place with all product suppliers and third-party service providers to ensure a mutual understanding about the protection of the client's personal information.

3.7 The Collector's suppliers, partners and clients will be subject to the same regulations as applicable to the Collector.

3.8 For purposes of this Policy, clients include potential and existing clients.

4 The use of Personal Information

4.1 The Client's personal information will only be used for the purpose for which it was collected as set out in more detail under clause 3.2 and as agreed to.

4.2 Read in conjunction with section 10 of the Act, and clause 2.4, Personal Information may only be collected if certain conditions, with supporting documentation, are met, as follows:

4.2.1 the client's consent to the processing: - consent is obtained from clients during the introductory, appointment and needs analysis stage of the relationship;

4.2.2 the necessity of processing: in order to conduct an accurate analysis of the client's needs;

4.2.3 processing complies with an obligation imposed by law on the Collector;

4.2.4 to conduct an affordability assessment if applicable;

4.2.5 processing protects a legitimate interest of the client; or

4.2.6 processing is necessary for pursuing the legitimate interests of the Collector or of a third party to whom information is supplied.

5 Disclosure of Personal Information

5.1 The Collector may disclose a client's personal information to any of the Collector's subsidiaries, joint venture companies and or approved product supplier or third-party service providers whose services or products clients elect to use. The Collector has agreements in place to ensure compliance with confidentiality and privacy conditions.

5.2 The Collector may also disclose a client's information where it has a duty or a right to disclose in terms of applicable legislation, the law, or where it may be deemed necessary in order to protect the Collector's rights.

5.3 All employees have a duty of confidentiality in relation to the Collector and clients.

5.4 Information on clients: Our clients' right to confidentiality is protected in the Constitution and in terms of the Law. Information may be given to a third party if the client has consented in writing to that person receiving the information.

5.5 The Collector views any contravention of this policy very seriously and employees who are guilty of contravening the policy will be subject to disciplinary procedures, which may lead to the dismissal of any guilty party.

6. Safeguarding Personal Information

6.1 It is a requirement of the Act to adequately protect personal information. The Collector will continuously review its security controls and processes to ensure that personal information is properly safeguarded.

6.2 The Collector's Information Officer is responsible for the compliance of the conditions of the lawful processing of personal information and other provisions of the Act. The Information Officer will be assisted by Deputy Information Officer(s).

6.3 This policy has been put in place throughout the Collector and training on this policy and the Act has already taken place and will continue to be conducted by the Collector.

6.4 Each new employee, where these provisions are relevant, who pertinently through their employment is required to Process Personal Information, will be required to sign an Employment Contract containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of the Act.

6.5 Every employee currently employed within the Collector will be required to sign an addendum to their Employment Contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of the Act.

6.6 All the Collector's electronic files or data are backed and stored off site.

6.7 The Collector's product suppliers, insurers and other third-party service providers will be required to sign a service level agreement guaranteeing their commitment to the Protection of Personal Information; this is however an ongoing process that will be evaluated as needed.

7. Correction of Personal Information

7.1 Clients have the right to access the personal information the Collector holds about them. Clients also have the right to ask the Collector to update, correct or delete their personal information on reasonable grounds. Once a client objects to the processing of their personal information, the Collector may no longer process their personal information.

7.2 The Collector will take all reasonable steps to confirm its clients' identity before providing details of their personal information or making changes to their personal information.

8. **Amendments to this Policy**

8.1 Amendments to, or a review of this Policy, will take place on an ad hoc basis or at least once a year.

9. **Access to Documents**

9.1 All company and client information must be dealt with in the strictest confidence and may only be disclosed, without fear of redress, in the following circumstances:

9.1.1 where disclosure is under compulsion of law;

9.1.2 where there is a duty to the public to disclose;

9.1.3 where the interests of the Collector require disclosure; or

9.1.4 where disclosure is made with the express or implied consent of the client.

10. **Requests for the Collector's Information**

10.1 This is dealt with in terms of the Promotion of Access to Information Act, 2 of 2000 ("PAIA"), which gives effect to the constitutional right of access to information held by the State or any person (natural and juristic) that is required for the exercise or protection of rights. Private bodies, like the Collector, must however refuse access to records if disclosure would constitute an action for breach of the duty of secrecy owed to a third party.

10.2 In terms hereof, requests must be made in writing on the prescribed form to the Information Officer in terms of PAIA. The requesting party must state the reason for wanting the information and has to pay a prescribed fee.

10.3 The Collector's manuals in terms of PAIA, which contains the prescribed forms and details of prescribed fees, is available from the Collector.

10.4 Confidential company and/or business information of the Collector may not be disclosed to third parties as this could constitute industrial espionage. The affairs of the Collector must be always kept strictly confidential.

11. **Retention of Documents**

11.1 'Hard Copy' - The statutory periods for the retention of documents are as per the Law. There are no hard copies available unless specifically provided for.

11.2 'Electronic Storage' - The internal procedure requires that electronic storage of information: important documents and information must be referred to and discussed with Human Resources, after which the Research and Development Department will arrange for the indexing, storage and retrieval thereof. This will be done in conjunction with the departments concerned.

11.3 Scanned documents: If documents are scanned, the hard copy must be retained for as long as the information is used or for 1 year after the date of scanning, apart from documents pertaining to personnel. Any document containing information on the written particulars of an employee, including employee's name and occupation, time worked by each employee, remuneration and date of birth of an employee under the age of 18 years; must be retained for a period of 3 years after termination of employment.

11.4 Section 51 of the Electronic Communications Act 25 of 2005 requires that personal information and the purpose for which the data was collected must be kept by the person who electronically requests, collects, collates, processes or stores the information and a record of any third party to whom the information was disclosed must be retained for a period of 1 year or for as long as the information is used.

11.5 It is also required that all personal information which has become obsolete must be destroyed.

12. Destruction of Documents

12.1 Documents may be destroyed after the termination of the retention period specified in terms of the Law. Research and Development will request departments to attend to the destruction of their documents and these requests shall be attended to as soon as possible.

12.2 Each department is responsible for attending to the destruction of its documents, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and to ascertain if there are important original documents in the file. Original documents must be returned to the holder thereof, failing which, they should be retained by the Collector pending such return.

12.3 After completion of the process in clause 12.2 above, the General Manager of the department shall, in writing, authorise the removal and destruction of the documents in the authorisation document. These records will be retained by Human Resources.

12.4 The documents are then made available for collection by the removers of the Collector's documents, who also ensure that the documents are shredded before disposal. This also helps to ensure confidentiality of information.

12.5 Documents may also be stored off-site, in storage facilities approved by the Collector.

13. Cross-Border Flow of Information

13.1 Section 72 of the Act provides that Personal Information may only be transferred out of the Republic of South Africa if the:

13.1.1 recipient country can offer such data an “adequate level” of protection. This means that its data privacy laws must be substantially like the Conditions for Lawful Processing as contained in the Act; or

13.1.2 the client or customer consents to the transfer of their personal information; or

13.1.3 transfer is necessary for the performance of a contractual obligation between the client or customer and the Collector; or

13.1.4 transfer is necessary for the performance of a contractual obligation between the Collector and a third party, in the interests of the client or customer; or

13.1.5 the transfer is for the benefit of the client or customer, and it is not reasonably practicable to obtain the consent of the client or customer, and if it were, the client or customer, would likely provide such consent.