V1.0

NAME OF COMPANY: DINGLEY MARSHALL LEWIN INC.

2011/109108/21

(the "Company")

MANUAL

in terms of

Section 51 of

The Promotion of Access to Information Act 2 of 2000

Date of Compilation	23 December 2020

Date of last revision	23 December 2020

Contents

1. Introduction

1.1. Dingley Marshall Lewin is an incorporated entity which conducts business as a law firm. We provide general legal services which includes litigation, notarial, conveyancing, company, competition, matrimonial, labour, commercial, ICT, intellectual property and social media law to our clients.

2. Contact Details of Information Officer

Name of Private Body	Dingley Marshall Lewin Inc.
Information Officer (head of company)	Ryan Gavin Dingley
Deputy Information Officer	Paula Jane Kennedy-Smith
Street Address	1st Floor, 22 Dreyer Street, Claremont, Cape Town, 7708
Postal Address	P.O. Box 397, Bergvliet, 7864
Telephone Number	021 200 0770
Fax Number	-
Email	paula@dmllaw.co.za
Website Address	www.dmllaw.co.za

3. PAIA and POPIA

3.1. The Promotion of Access to Information Act 2 of 2000 ("PAIA") grants a requester access to records of a private body, if the record is required for the exercise or protection of any rights. If a public body lodges a request, the public body must be acting in the public interest.

3.2. The Protection of Personal Information Act 4 of 2013 ("POPIA") gives effect to the constitutional right to privacy. One of the data processing principles under POPIA is that of data subject participation, which allows for data subjects to access and correct their personal information held by a responsible party. This manual provides for data subject to request this information from the Company.

4. Requests for Information

4.1. Requests in terms of PAIA must be made in accordance with the prescribed procedures, at the prescribed rates provided. The forms and tariff are dealt with in Regulations 6 and 7 promulgated in terms of PAIA.

4.2. The information will only be made available subject to the provisions of PAIA and access to records may also be refused due to attorney-client privilege.

4.3. Proof of payment of the said prescribed fee must accompany the completed application form.

5. The Guide

5.1. Requesters are referred to the Guide in terms of Section 10 which has been compiled by the South African Human Rights Commission ("SAHRC"), which will contain information for the purposes of exercising Constitutional Rights. The Guide is available from the SAHRC in all of the official languages.

5.2. The contact details of the SAHRC are:

Postal Address	PAIA Unit, The Research and Documentation Department, Private Bag 2700, Houghton, 2041
Telephone Number	+27 11 877 3600
Fax Number	+27 11 403 0625
Email Address	PAIA@sahrc.org.za
Website	www.sahrc.org.za

6. Latest notice in terms of Section 52(2) (if any)

6.1. At this stage no notice has been published on the categories of records that are automatically available without a person having to request access in terms of PAIA.

7. Information Available in terms of any other Legislation

Information is held and maintained by the Company in compliance with the following legislation:

- Administration of Estates Act, No. 66 of 1965
- Arbitration Act No. 42 of 1965
- Basic Conditions of Employment No. 75 of 1997
- Broad Based Black Economic Empowerment Act No. 53 of 2003
- Companies Act No. 71 of 2008
- Compensation for Occupational Injuries and Health Diseases Act No.130 of 1993
- Consumer Protection Act No. 68 of 2008
- Copyright Act No. 98 of 1978
- Electronic Communications Act No. 36 of 2005
- Electronic Communications and Transactions Act No. 25 of 2002
- Employment Equity Act No. 55 of 1998
- Financial Intelligence Centre Act No. 38 of 2001
- Income Tax Act No. 95 of 1967
- Insurance Act No 27 of 1943
- Intellectual Property Laws Amendments Act No. 38 of 1997
- Labour Relations Act No. 66 of 1995
- Legal Practice Act No. 28 of 2014
- Long Term Insurance Act No. 52 of 1998
- National Credit Act No. 34 of 2005
- Occupational Health & Safety Act No. 85 of 1993
- Prescription Act No. 68 of 1969
- Prevention and Combating of Corrupt Activities Act No. 12 of 2004

- Prevention of Organized Crime Act No. 121 of 1998
- Protection of Personal Information Act No. 4 of 2013
- Short Term Insurance Act No. 53 of 1998
- Skills Development Act No. 97 of 1998
- Skills Development Levies Act No. 9 of 1999
- Trademarks Act No. 194 of 1993
- Unemployment Contribution Act No. 4 of 2002
- Unemployment Insurance Act No. 30 of 1996
- Value Added Tax Act 89 of 1991

8. Schedule of Records of the Company

The records held by the Company, both those that can be accessed without an application in terms of PAIA and otherwise, are listed in Schedule 1.

9. Schedule of Personal Information Processed by the Company

9.1. *Schedule of Personal Information.* The personal information processed by the Company in terms of POPIA is set out in Schedule 2.

9.2. *Planned and actual transborder flows of personal information.* The Company may use hosting or cloud services to store and process personal information that are not located in the RSA. If it does so, it will ensure that the level of protection given to the personal information is at least as good as that provided for under RSA Law, either by means of a binding contract with the service provider, or by using a service provider located in a country with privacy laws of similar or stronger effect.

9.3. Information Security Measures.

The Company employs appropriate, reasonable technical and organisational measures to secure the integrity and confidentiality of personal information in its possession or under its control, which include the following:

9.3.1. Ensuring physical security measures are in place at all times, including, but not limited to, having an alarm system in place; locking of all doors to the office;

9.3.2. Keeping all physical client files (including FICA documentation) in cabinets located in access-controlled offices;

9.3.3. Archiving client files securely with a third party storage services provider;

9.3.4. Backing up and storing all client information and files to the password protected cloud storage provided by Microsoft and protected by security processes set up by Microsoft;

9.3.5. Shredding of all client information and files once closed and digital backups made;

9.3.6. Ensuring each desktop computer used by staff is password protected;

9.3.7. Ensuring each laptop computer used by staff is password protected and encrypted;

9.3.8. Ensuring firewall and anti-virus software is installed on all computers and laptops and running at all times;

9.3.9. Identifying reasonably foreseeable internal and external risks to personal and other information in its possession or under its control;

9.3.10. Establishing and maintaining appropriate safeguards against the risks identified;

9.3.11. Regularly verifying that the safeguards are effectively implemented;

9.3.12. Ensuring that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards;

9.3.13. Ensuring compliance by all staff of its strict security policy contained in its Electronic Communications Policy, which includes that:

9.3.13.1. All information relating to the Company's clients and business operations, whether paper-based or electronic, is confidential and must be treated with utmost care;

9.3.13.2. Staff are strictly prohibited from performing any act which may damage or threaten the functioning, security and/or integrity of the Company's electronic communications system;

9.3.13.3. Staff must:

- Maintain exclusive control over and use of any password or access code used to gain access to the electronic communications system, and protect it from inadvertent disclosure to others;
- Take care not to open any unsolicited messages or messages from senders unknown, especially when such messages include attachments;
- Ensure that the information or data under their control is properly safeguarded according to its level of sensitivity;
- Make back-ups of all sensitive, critical and valuable data files as often as is deemed reasonable by the system controller;
- Keep all confidential information secure and use it only for the purposes intended and not disclose it to any unauthorised third party;
- When working remotely, password protect any work which relates to the Company's business in order to prevent unauthorised access thereof.
- Install (or allow the IT service provider to install) and run backup software on devices if provided to them by the Company for business use;
- Install and use virus detection software on any device connected to the Company's electronic communications system; and

- Not use knowledge of passwords, codes or loopholes in the Company's electronic communications system to damage resources, obtain extra resources, take resources from other users, gain unauthorised access to other parts of the system or otherwise make use of the system in a manner for which proper authorisation has not been given;

9.3.13.4. Copies of confidential information should be printed out only as necessary, retrieved from the printer immediately, and stored or destroyed in an appropriate manner;

9.3.13.5. If any sensitive or confidential information is lost or disclosed to unauthorised parties, or suspected to be lost or disclosed to unauthorised parties, the system controller must be notified immediately; and

9.3.13.6. Any incident that appears or is likely to compromise the security of the Company's electronic communications system must be reported to the system controller or the IT service provider. This will include missing data, virus infestations, and unexplained transactions.

10. Other Prescribed Information

10.1. At the time of the compilation of this manual, no further information has been prescribed.

11. Availability of Manual

11.1. This manual is available free of charge for inspection at the above-mentioned address; and at the South African Human Rights Commission.

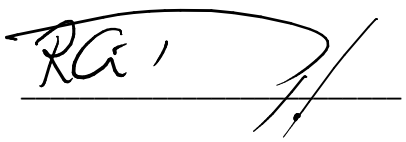
11.2. Copies of the manual may be obtained, subject to the prescribed fees.

11.3. The manual may also be accessed on the Company's website or alternatively a copy is available upon request directly from the SAHRC.

12. Reservation of Rights

12.1. Nothing in this manual is to be construed as a waiver of the right to the confidentiality of any document or any legal privilege or right of non-disclosure attaching to any document mentioned herein, whether in terms of any statute or under the common law. All rights in this regard are fully reserved.

----------ooOoo----------



Signature by Head of Institution

Schedule 1 – Records Available in Terms of PAIA

Category	Subject	Availability
Communication	Public product information	**Available**
	Media releases	**Available**
	Promotion of Access to Information Act Manual	**Available**
	Internal and external correspondence	**May not be disclosed**
	News and publications	**Available**
Human Resources	Employment contracts	**May not be disclosed**
	Disciplinary records	**May not be disclosed**
	Employment equity plan	**Limited disclosure only on request**
	Skills development programme	**Limited disclosure only on request**
	Salaries and wages records	**May not be disclosed**
	Documents relating to employee benefits	**May not be disclosed**
	Disciplinary code	**Limited disclosure only on request**
	Personnel Guidelines, Policies and Procedures	**Limited disclosure only on request**
	Leave records	**May not be disclosed**

	Personal information of past, present and prospective employees and officer / directors	**May not be disclosed**
	Banking details	**May not be disclosed**
	PAYE records	**May not be disclosed**
	Documents issued to employees for income tax purposes	**May not be disclosed**
	Records of payments made to SARS on behalf of employees	**May not be disclosed**
	UIF records	**May not be disclosed**
Client Records	Records provided by clients, including documentary information required in compliance with FICA	**May not be disclosed**
	Records provided by a client to a third party acting for and on behalf of the Company	**May not be disclosed**
	Records provided by third parties	**May not be disclosed**
	Client files, including correspondence with clients	**May not be disclosed**
	Correspondence with third parties	**May not be disclosed**
	Fee agreements, quotations and mandates	**May not be disclosed**
Immovable and Movable Property	Asset register	**Limited disclosure only on request**
	Agreements for the lease of immovable property	**May not be disclosed**

	Agreements for the lease or sale of movable property	**May not be disclosed**
	Credit sale agreements and/or hire purchase agreements	**May not be disclosed**
	Other agreements for the purchase, ordinary sale, conditional sale or hire of assets	**May not be disclosed**
Financial Information	Financial and accounting records	**May not be disclosed**
	Banking details	**Available upon request**
	Insurance records	**May not be disclosed**
	Tax compliance documents and tax returns	**May not be disclosed**
	Accounting records	**May not be disclosed**
	Bank statements	**May not be disclosed**
	Invoices in respect of creditors and debtors	**May not be disclosed**
	Details of auditors	**Available upon request**
	Auditors' reports in respect of audits conducted	**Limited disclosure only on request**
Information Technology	Computer software, support and maintenance agreements	**May not be disclosed**
	Other documentation pertaining to computer systems and computer programmes	**May not be disclosed**
Information relating to legal proceedings	Records relating to legal proceedings involving the Company	**May not be disclosed**
General Records	Client, supplier and document databases	**May not be disclosed**

	Legal Practice Council records, including Fidelity Fund Certificate	**Limited disclosure only on request**
	BBBEE Certificate	**Available upon request**
	Commercial agreements	**May not be disclosed**
	Statutory records	**Available upon request**
	Organisational structure	**Available upon request**
Intellectual Property	List of trademarks, copyrights and designs held and pending applications	**Available upon request**
	Records relating to domain names	**Available upon request**
	Licenses relating to intellectual property rights	**Limited disclosure only on request**
Company Records	Documents of incorporation	**Available upon request**
	Memorandum and Articles of Association	**Limited disclosure only on request**
	Minutes of Board of Directors meetings	**May not be disclosed**
	Records relating to the appointment of directors/ auditor/ secretary/ public officer and other officers	**May not be disclosed**
	Share Register and other statutory registers	**May not be disclosed**

----------ooOoo----------

Schedule 2 – Personal Information Processed in Terms of POPIA

Personal Information	**Purpose of Processing**	**Data Subjects it relates to**	**Valid Recipients**
Employee Personal Information, including: - Full name - Identity Number - Physical address - Cellphone number - Personal Email address - Banking details - Tax information	Managing employment relationship. As required by statutory obligations in terms of the relevant employment legislation. As required by SARS for tax purposes.	Past and current employees of the company.	Management of the Company. Accounts department of the Company. SARS. Statutory bodies and courts in terms of legislation or court orders.
Supplier and Third-Party Contractors' Personal Information, including: - Full name - Identity Number - Company name - Company Registration Number - Physical address - Contact details - VAT number - Banking details	Managing supplier/contractor relationship for services to be provided. To make payments for services rendered. As required by statutory obligations in terms of the relevant legislation.	Past and current suppliers/contractors of the Company.	Management of the Company. Accounts department of the Company. SARS. Statutory bodies and courts in terms of legislation or court orders.
Client Personal Information, including: - Full name - Identity Number	Managing client relationship. To render legal services to client.	Past and current clients of the Company.	Management of the Company.

- Company/Entity name - Company/Entity Registration Number - Company/Entity incorporation documentation - Physical address - Contact details - VAT / Income Tax number - Banking details - Documentation / information provided by the client relating to their legal matter	To comply with obligations in terms of FICA. To make payments to client where required. As required by statutory obligations in terms of the relevant legislation.		Financial Intelligence Centre. Staff working on the client's matter. Accounts department of the Company. Courts where the client's matter is to be heard. Third party suppliers like correspondent attorneys. Opposing attorney, with consent of the client. SARS. Statutory bodies and courts in terms of legislation or court orders.
Personal Information collected from COVID19 sign-in register	Required to be obtained and kept in accordance with the relevant Regulations in terms of the Disaster Management Act.	Any person entering the Company's office.	Management of the Company. Statutory bodies and courts in terms of legislation or court orders.

Personal Information obtained from contact requests or queries submitted on the Company's website, including: - Name - Cellphone number - Email address	Used to contact the prospective client about the query.	Any person submitting a contact request or query on the Company's website.	Management of the Company. Staff dealing with the contact request or query. Statutory bodies and courts in terms of legislation or court orders.

----------ooOoo----------