POPIA MANUAL

BRADBURY FINANCE (PTY) LIMITED

(REGISTRATION NUMBER: 2009/004295/07)

("*THE COMPANY*")

1. INTRODUCTION

1.1. The Protection of Personal Information Act, 4 of 2013, ("POPIA"), provides for protection principles that the Company must comply with to protect the Personal Information of all Data Subjects. Should a person require access to these Personal Information, then access is allowed in terms of the Promotion of Access to Information Act, 2 of 2000 ("PAIA").

1.2. PAIA gives effect to section 32 of the Constitution, which provides access to Personal Information if a person wants to exercise a right or to protect a right, subject to the procedural requirements laid down by PAIA.

1.3. Section 10 of POPIA provides that the Company must implement a Manual that must comply with section 14 and 51 of PAIA, that should be made available to persons who want to access the Company's Personal Information.

This POPIA Manual is available for inspection by contacting the Companies and the South Africa Human Rights Commission at the contact details provided below.

2. PURPOSE

2.1. <u>This purpose of the Manual is to:</u>

2.1.1. provide details on records and information of the Company that are available and accessible once the requirements for access have been met; and

2.1.2. sets out the procedures to be followed by a person that wants access to the Personal Information that is subject to protection and non-disclosure in terms of POPIA, if such person wants to exercise or to protect a right.

2.2. The Manual is available for inspection at the Company's offices at no cost, and, also on the website www.bradburyfin.co.za

3. AVAILABLE INFORMATON

The information provided below is regarded as available information, however currently no notice has been published in terms of section 52(2) on the categories of records that will automatically be available without following the required processes provided for in terms of this POPIA Manual.

Please note that the inclusion of any subject or category of records in this POPIA Manual does not mean that information or records falling withing those subjects and/or categories will automatically be made available. Certain grounds of refusal may apply to a request for such record.

Company Name	Bradbury Finance (Pty) Limited		
Registration no	Specified above	**>*COMPANY*< no**	Specified above
CEO	Lee-Ann Wijtenburg	**Key Individual**	Lee-Ann Wijtenburg
Structure	Western Cape head office		
Functions	The Company is in the financial sector, providing financial services		
Postal address	Bradbury House, 31A Bright Street Somerset West		
Business/ Street Address	Bradbury House, 31A Bright Street Somerset West		
Phone Number	+27 21 851 6537	**Website**	www.bradburyfin.co.za
Information Officer	Lee-Ann Wijtenburg	**Email address**	lee@bradburyfin.co.za
Deputy Information Officer/s	Lee-Ann Wijtenburg	**Email address**	lee@bradburyfin.co.za
SA Human Rights Commission (SAHRC) Guide	The SAHRC Guide can be obtained from the SA Human Rights Commission at no cost: Address: PAIA Unit, The Research & Document Dept, Private Bag x2700, Houghton, 2041 Tel: +27 11 877 3600; Facsimile: +27 11 403 0625; Website: www.sahrc.org.za		

APPLICABLE LEGISLATION

The Company's' operations and information is available in accordance with the following legislation, including but not limited to:

- Basic Conditions of Employment Act 75 of 1997
- The Companies Act 71 of 2008
- Consumer Protection Act 68 of 2008
- Collective Investment Schemes Control Act 45 of 2002
- Credit Rating Services Act 24 of 2012
- Employment Equity Act 55 of 1998
- Financial Advisory and Intermediaries Services Act 37 of 2002
- Financial Institutions (Protection of Funds) Act 28 of 2001
- Financial Intelligence Centre Act 38 of 2001
- Financial Markets Act 19 of 2012
- Financial Sector Regulation Act 9 of 2017
- Financial Services Board Act 97 of 1990
- Financial Services Ombud Schemes Act 37 of 2004
- Financial Supervision of the Road Accident Fund Act 8 of 1993
- Friendly Societies Act 25 of 1956

- Income Tax Act 95 of 1967
- Insurance Act 18 of 2017
- Labour Relations Act 66 of 1995
- Long-term Insurance Act 52 of 1998
- Occupational Health and Safety Act 85 of 1993
- Pension Funds Act 24of 1956
- Protection of Personal Information Act 4 of 2013
- Short-term Insurance Act 53 of 1998
- Skills Development Act 97 of 1998
- Skills Development Levies Act 9 of 1999
- Unemployment Contributions Act 63 of 2001
- Value Added Tax Act 89 of 1991

SUBJECTS AND CATEGORIES OF RECORDS HELD BY THE COMPANY	
Statutory Company Information	- The Memorandum and Articles of Association - Memorandum of Incorporation - Certificate of Incorporation - Records of all subsidiary Company's - The shares register. - Shareholders' agreements. - Minutes of general meetings of the shareholders. - Register or list of directors. - Minute books and internal resolutions. - Power of attorney agreements and a list of persons authorised to bind the Company's - Statutory registers, including a register of bonds and pledges, and a register of directors' interests in contracts.
Financial and Tax Records	- Accounting records, books and documents. - Interim and annual financial reports. - Auditor's details. - External auditors' reports. - Details of actuaries of the pension scheme of the >*COMPANY*<. - Tax returns. - PAYE records - Skills Development Levies records - Other documents and agreements relating to taxation.
Banking Details	- Bank facilities and account details. - Bank statements. - Guarantees given by, or in respect of, the Company's
Human Resources / Employment Records	- List of employees and/or contractors. - Contracts of employment with directors, officers and employees. - Services agreements with independent contractors and outsource partners. - Expenditure or reimbursement agreements with directors. - Documents relating to employee benefits. - Compensation or redundancy payments. - Documents and information in respect of share incentive schemes or trust. - Personnel files. - Employee code of conduct. - Employment equity plan. - Procedural agreements and policies.

	- Disciplinary records and documentation pertaining to disciplinary proceedings. - CCMA records. - Training manuals. - Other information relating to employees of the Companies - Confidentiality agreements
Licenses and authorisations	- Regulatory authorisations, other authorisations, licenses, material permits, consents, approvals, and certificates. - Applications for licenses and permits. - Registrations and declarations of permits.
Insurance	- Insurance policies taken out for the benefit of the Company's. - Claims records
Immovable and movable property	- Title deeds of land owned by the Company. - Agreements for the lease or sale of land and/or other immovable property by the Company. - Agreements for the lease or sale of movable property by the Company. - Mortgage bonds, *liens*, notarial bonds or security interests on property. - Other agreements for the purchase, ordinary sale, conditionalsale, or hire of assets.
Information Technology	- Computer software support and maintenance agreements. - Web site development, support and maintenance agreements. - Computer software license agreements. - Agreements in respect of computer hardware used by the Company. - Agreements with Internet Service Providers and other telecommunications entities. - Leased line agreements. - Other documentation pertaining to computer systems and computer programs held by the Company. - Individual contracts in respect of usage of cellular telephones. - SITA agreements.
Specific Agreements Relating to the Business Activities	- Indemnity, confidentiality and non-disclosure agreements. - Regulatory agreements. - Agreements relating to transactions. - Presentations to clients.
Miscellaneous agreements	- Loans from third parties (including banks). - Loans to third parties. - Suretyship agreements. - Agreements restricting the trading activities of the Company. - Agency, management and distribution agreements. - Royalty agreements. - Agreements in terms of which the Company is a member of a joint venture, consortium, partnership, incorporated or unincorporated association, and shareholders' agreements of another entity which the Company is party to. - Any other agreements.
Policy documents	- Governance policy. - Risk management policy - Human Resources policy. - Treating Customers Fairly. - Privacy and Data Protection Policy. - Complaints Policy.

Procedures	- Standard operating procedures - Disciplinary procedures -
Correspondence	Correspondence including internal and external memoranda
Legal proceedings	- Records relating to legal proceedings. - Records relating to arbitration matters.
Clients	- Agreements with clients - Service Level Agreements - Broker Agreements. - Business strategies - Advice records - Financial Needs Analysis. - Client Mandate - Discretionary Mandate - Applications. - Investment Risk Profiles. - Claims records - Complaints and outcomes - Assets under management records - Financial records - FICA documentation - Contact lists - Agendas and minutes of meetings - Product brochures. - Marketing plans - Letters/sheets - Client briefs - Client E-mails - Telephone recordings - Registers

4. PROCEDURES TO FOLLOW FOR ACCESS TO INFORMATION

4.1. REQUESTER

4.1.1. **Personal Requester:**

A Personal Requester is a requester who is seeking access to a record containing Personal Information about the Requester itself. Access will be granted by the Company's subject to applicable legislation.

4.1.2. **Other Requester**:

If a person other than the Personal Requester is seeking access to a record containing Personal Information, then the Company are not obliged to grant access to such record, unless such person fulfils the requirements for access as provided for in terms of PAIA.

4.2. **FEES PAYABLE**

The applicable fees are prescribed in terms of the Regulations promulgated under PAIA:

4.2.1. **Request fee:** This does not apply if the request is for personal records of the person requesting – in this instance no fee is payable.

4.2.2. **Access fee:** An access fee is payable prior to being granted access to the records in the form required. These fees are prescribed in Part III of Annexure A as defined in Government Gazette Notice No. 187, Regulation 11.

4.3. **REQUEST PROCEDURES**

4.3.1. Access to records with Personal Information is subject to the procedural requirements contained in PAIA.

4.3.2. A Requester must complete the prescribed form enclosed herewith in Appendix 1 and payment of the required fee (only if it is an Other Requester) must be made.

4.3.3. The completed and signed Appendix 1 form together with proof of payment must either be posted, submitted per hand or be emailed to the Information Officer at the email address stated above.

4.3.4. If an individual is unable to complete the prescribed form because of illiteracy or disability, such a person may make the request orally to the Information Officer.

4.3.5. If a request is made on behalf of another person, the Requester must then submit proof of the capacity in which the Requester is making the request on behalf of the other person to the satisfaction of the Information Officer.

4.3.6. All required information must be provided on the Appendix 1 form, and the information must be true complete and correct with enough particularity to enable the Information Officer to identify:

4.3.6.1. the Requester's identity;

4.3.6.2. contact details of the Requester;

4.3.6.3. the requested record/s, and

4.3.6.4. the form of access required by the Requester.

4.3.7. A Requester may only request access to a record in order to exercise or protect a right and must clearly state what the nature of the right is so to be exercised or protected. The requester is further

required to provide an explanation of why the requested record is required for the exercise or protection of that right.

4.3.8. The Company will process a request to access a record within 30 (thirty) days of receipt of the completed Appendix 1 form together with proof of payment, if applicable, unless the Requestor has stated exceptional reasons and circumstances together with proof, if applicable, that would satisfy the Information Officer that the time period not be complied with.

4.3.9. The Company shall inform the Requester in writing whether access has been granted or denied together with reasons thereof.

4.3.10. If the Requester requires access to the records in another manner, the Requester must state the manner and the particulars so required.

4.4. **GROUNDS FOR REFUSAL**

PAIA provides several grounds on which a request for access to information must be refused and a complete list of the grounds for refusal is available in Chapter 4 of PAIA.

4.4.1. <u>These grounds mainly concern instances that may include where:</u>

4.4.1.1. the privacy and interests of other individuals are protected;
4.4.1.2. such records are already otherwise publicly available;
4.4.1.3. public interests are not served;
4.4.1.4. the mandatory protection of commercial information of a third party;
4.4.1.5. the mandatory protection of certain confidential information of a third party.

5. THE PROTECTION OF PERSONAL INFORMATION ACT (POPIA) GUIDE

DEFINITIONS

The following definitions have the meanings as defined in terms of section 1 of POPIA and are detailed below:

<u>Data Subject:</u> means the person to whom the personal information relates.

<u>Responsible Party:</u> The entity which determines the purpose of and means for processing personal information.

<u>Operator:</u> The company or a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of the responsible party.

Personal Information: means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person.
- information relating to the education or the medical, financial, criminal or employment history of the person.
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;
- the views or opinions of another individual about the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.
- Special Personal Information includes:
  religious or political beliefs
  race or ethnic origin
  trade union membership
  political opinions
  health, sexual life
  criminal behavior.

Processing: means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;

- dissemination by means of transmission, distribution or making available in any other form; or

- merging, linking, as well as restriction, degradation, erasure or destruction of information.

Direct Marketing: means the use of personal information for the purposes of direct marketing by means ofany form of electronic communication.

6. EXCLUSIONS

POPIA protection does not apply to the following information:

The processing of personal information:

- in the course of purely personal or household activity.
- that has been de-identified to the extent that it cannot be re-identified again.
- by or on behalf of a public body —
  - which involves national security, including activities that are aimed at assisting in the identification of the financing of terrorist and related activities, defense or public safety; or
  - the purpose of which is the prevention, detection, including assistance in the identification of the proceeds of unlawful activities and the combating of money laundering activities, investigation or proof of offences, the prosecution of offenders or the execution of sentences or security measures, to the extent that adequate safeguards have been established in legislation for the protection of such personal information;

- by the Cabinet and its committees or the Executive Council of a province; or

- relating to the judicial functions of a court referred to in section 166 of the Constitution of the Republic of South Africa, 1996.

''***Terrorist and related activities***'', for purposes of subsection (1)(c), means those activities referred to in section 4 of the Protection of Constitutional Democracy against Terrorist and Related Activities Act, 2004 (Act No. 33 of 2004).

7. The Data subject consent is required, but not if it would prejudice a lawful purpose, or the information is publicly available.

7.1.1. PROCESSING OF PERSONAL INFORMATION WITHIN THE COMPANY

The Company is Processing the Personal Information of its Data Subjects as follows:

Purpose of processing:	- Rendering of financial services to clients - Provision of value-added services - Maintain accounts and records - Support and manage employees - Use of CCTV systems to prevent and detect crime - Assessment and processing of claims - Fraud prevention & detection - Market research and statistical analysis - Compliance with legal and regulatory requirements - Verifying identity
Data subject categories:	- Shareholders - Board members - Directors - Employees - Consultants - Complainants & enquirers - Trustees - Employers and employees of other organisations - Subsidiary Company's - External Company's / contractors - Suppliers and service providers - Clients and their members / policyholders / subscribers - Individuals captured by CCTV images / video - Individuals who have indicated an interest in our products / services
Types/ classes of information processed	- Personal details - Business activities - Products / services provided - Personal views / preferences - Family details - Education & employment details - Visual images of individuals captured on CCTV - Financial details - Racial / ethnic origin - Trade union membership - Offences / alleged offences - Religious or other beliefs - Physical / mental health details - Criminal proceedings, outcomes & sentences
Who the information may be shared with	It is sometimes necessary to share Personal Information with individuals and/or with other organisations. Where this is necessary, the Company are required to comply with all aspects of POPIA. The following are types of organisations which the Company may need to share some of the Personal Information it processes. Only where it is necessary or required Personal Information may be shared with:

	- Family, associates and representatives of the person whose Personal Information we are processing - Employment and recruitment agencies - Financial organisations - Credit reference agencies - Healthcare, social and welfare organisations - Healthcare professionals - Regulatory authorities - Central government - Police / courts where necessary - Business associates - Claimants / beneficiaries - Persons making an enquiry / complaint - Private investigators - Educators and examining bodies - Claims investigators - Suppliers and service providers - Industry bodies - Ombudsman - Legal Advisors, Compliance Officers, advocates or attorneys - Auditors - Tax Consultants - IT Services Providers - Debt collection and tracing agencies - Other Companies in the group - Pension fund administrators - Trade unions - Security organisations -
Cross border flows of Personal Information	It may be necessary to share Personal Information of Data Subjects with third parties in other countries subject to compliance with POPIA. This will only be done if one of the following requirements is met: - The third party who is the recipient of the information is subject to a law, bindingcorporate rules or binding agreement which provide an adequate level of protection that— • effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawfulprocessing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person, as set out in the Protection of Personal Information Act; and • includes provisions that are substantially similar to this section, relatingto the further transfer of personal information from the recipient to thirdparties who are in a foreign country. - The data subject consents to the transfer. - The transfer is necessary for the performance of a contract between the data subject and the company in question, or for the implementation of pre- contractual measures taken in response to the data subject's request. - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the company in questionand a third party; or - The transfer is for the benefit of the data subject, and— • it is not reasonably practicable to obtain the consent of the data subject to that transfer; and • if it were reasonably practicable to obtain such consent, the datasubject would be likely to give it.

7.1.2. **PERSONAL INFORMATION PROTECTION PRINCIPLES FOR RESPONSIBLE PARTIES**

The Company's comprehensive Data Protection Policies and procedures in place in order to comply with principles of POPIA and ensure that the best efforts are employed to ensure the protection of Personal Information. The Company has implemented the required controls and employ up to date technology to ensure the protection, confidentiality, integrity and availability of the Personal Information that it processes.

7.1.2.1. **Accountability:**

The Responsible Party must ensure compliance. The Responsible Party is required to audit the processes used to collect, record, store, disseminate and destroy personal information: in particular, ensure the integrity and safekeeping of personal information in your possession or underyour control. The Responsible Party must take steps to prevent the information being lost or damaged, orunlawfully accessed.

7.1.2.2. **Purpose Specification:**

The Responsible Party must define the purpose of the information gathering and processing: personal information must be collected for a specific, explicitly defined and lawful purpose that isrelated to a function or activity of the company concerned.

7.1.2.3. **Processing Limitation:**

- The Responsible Party must ensure processing is lawful and:
- done in a reasonable manner that does not infringe the privacy of the Data Subject.
- adequate, relevant and not excessive given the purpose.
- must have obtained consent or it must be necessary.
- If consent is obtained then it must be voluntary, specific and informed.

7.1.2.4. **Take steps to notify the Data Subject:**

The individual whose information is being processed has the right to know this is being done

The Data Subject must be informed about:

- the name and address of the company processing their information.
- he or she must be informed as to whether the provision of the information is voluntary or mandatory.

8. **Further Processing Limitation:**

Assess whether further processing is permitted, one must ask the following questions:

8.1. Is there a valid relationship between the purposes?

8.2. What is the nature of information?

8.3. What are the consequences for data subject?

8.4. The manner in which information was collected?

8.5. Are there any contractual rights between the parties?

9. **Review the rationale for any further processing, asking for the following**:

If information is received via a third party for further processing, this further processing must be compatible with the purpose for which the data was *initially* collected.

10. **Information quality:**

10.1. The Responsible Party must take reasonably practicable steps to ensure that the information is complete, accurate, not misleading; and updated where necessary.

10.2. The Responsible Party must notify Information Regulator once POPIA is enacted and Register with the Information Regulator.

10.3. The Responsible Party must take reasonable steps to notify the Data Subject of:

10.3.1. Information being collected;

10.3.2. Purpose for which information is collected;

10.3.3. Whether the supply of information is voluntary or mandatory;

10.3.4. The consequences of failure to provide information; and

10.3.5. Any particular law that applies

11. **Accommodating Data Subject requests:**

POPIA allows for Data Subjects to make certain requests, *free of charge*, to organisations that holds their Personal Information. An example is where the Data Subject has the right to know the identity of all third parties that have had access to their information. A Data Subject may also ask for a record of the Personal Information concerned.

12. **Security:**

12.1. The Responsible Party is required to *secure the integrity of personal information* by takingappropriate, reasonable technical and organisational measures to prevent:

12.1.1. Loss, damage or unauthorised access.

12.1.2. Unlawful access to or processing of personal information.

12.2. The Responsible Party must take all reasonable measures to:

12.2.1. Identify all reasonably foreseeable internal and external risks;

12.2.2. Establish and maintain appropriate safeguards against the risks;

12.2.3. Regularly verify that the safeguards are adequately implemented;

12.2.4. Ensure the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards

12.3. The Responsible Party must oversee an Operator who processes data on his/her behalf. Responsible Party must be aware of the following:

12.3.1. The Operator must treat information confidentially;

12.3.2. The Responsible Party must ensure that the operator establishes and maintains appropriate security safeguards;

12.3.3. ALL processing by an operator must be governed by a written contract;

12.3.4. In the event of security breaches, the Responsible Party must notify the Regulator and the data subject

13. **Retain records for required periods:**

13.1. Personal information must be destroyed, deleted or 'de-identified' as soon as the purpose of collecting the information has been achieved.

13.2. However, a record of the information must be retained if an organisation has used it to make a decision about the data subject. The record must be kept for a period long enough for the data subject to request access to it.

13.3. This requirement is subject to other legislation e.g. FAIS and FICA which provide for a period of 5 years to keep records.

14. **Cross Border Data Transfer:**

14.1. There are restrictions on the sending of personal information out of South Africa as well as on the transfer of personal information back into South Africa.

14.2. The applicable restrictions will depend on the laws of the country to whom the data is transferred or from where the data is returned.

14.3. The Responsible Party must assess the applicable laws and institute a written protocol to cover these requirements.

15. ROLES AND RESPONSIBILITIES OF OPERATORS

15.1. Duties of an Operator:

15.1.1. All Information processed by an operator must be treated in the following manner:

15.1.1.1. The Responsible party must be aware of the Operators processing.

15.1.1.2. The Operator must treat information confidentially.

15.1.1.3. The Responsible party must ensure that the Operator establishes and maintains appropriate security safeguards.

15.1.1.4. In the event of security breaches, the Operator via the Responsible party must notify the Regulator and the data subject.

15.1.1.5. The processing by an operator must be governed by a written contract between the Responsible party and the Operator.

15.2. Contents of the Contract:

The Contract between Operator and Responsible Party must detail at least the following:

15.2.1. the legitimate grounds for collecting and using personal data collected;

15.2.2. the lawful purpose for which data are being collected;

15.2.3. the limit of processing and prohibiting of further processing;

15.2.4. the extent of information that is required to prevent any excessive information collection;

15.2.5. the information retention periods and requirements applicable together with destruction processes and procedures;

15.2.6. the right of individuals to request such information and query the use thereof;

15.2.7. The security measures required to prevent the unauthorised or unlawful processing of personal data or access to personal data, including accidental loss or destruction or damage to personal data.

16. **DEALING WITH SPECIAL PERSONAL INFORMATION**

Note: If an objection is received from a Data Subject to process the Special Information, then this information may not be supplied to 3rd parties without the Data Subject's consent.

16.1. **Religious or Philosophical Beliefs** processingmay take place by Spiritual or religious organisations & institutions, provided that the information concerns data subjects belonging to such organisations; if it is necessary to achieve their aims and principles; or to protect the spiritual welfare of the data subjects.

16.2. **Race** processing may be carried out to Identify data subjects when this is essential and to Comply with laws or measures designed to protect or advance persons disadvantaged by unfair discrimination

16.3. **Trade Union Membership** processing may take place by a trade union to which the data subject belongs, or the trade union federation to which the trade union belongs, if the processing is necessary to achieve the aims of the trade union/trade union federation.

16.4. **Political Persuasion** processing may be undertaken by an institution founded on political principles if such processing isnecessary to achieve the aims or principles of the institution.

16.5. **Health or Sexual Life** processing must be confidential and may take place by:

16.5.1. Medical practitioners, healthcare institutions;

16.5.2. Insurance Companies, medical aid scheme providers;

16.5.3. Schools;

16.5.4. Institutions of probation, child protection or guardianship;

16.5.5. Pension funds and employers if processing is necessary for:

16.5.5.1. Implementation of laws/pension regulations; and

16.5.5.2. Re-integration/support for workers or persons entitled to benefit in connection with sickness/work incapacity

16.6. **Criminal behavior** processing may take place by:

16.6.1. Bodies charged by law with applying criminal law;

16.6.2. Responsible parties who have obtained the information in accordance with the law;

16.6.3. Responsible parties who process the information for their own lawful purposes to assess an application by the data subject in order to take a decision about or provide a service to thatdata subject to protect their legitimate interests in relation to criminal offences.

16.7. **General Exemptions**

16.7.1. The Regulator may authorise processing of any information, which will not be in breach of POPIA,if the public interest includes:

16.7.1.1. the legitimate interests of State security;

16.7.1.2. the prevention, detection and prosecution of offences;

16.7.1.3. important economic and financial interests of the State or, a public body;

16.7.1.4. historical, statistical or research activity.

17. DIRECT MARKETING BY MEANS OF UNSOLICITED ELECTRONICCOMMUNICATIONS

17.1. Direct marketing is prohibited unless you have consent, or the target is already a customer.

17.2. You may only approach a person for consent once and if they have not previously withheld such consent.

17.3. You may only use the information for the purpose it was obtained, for a customer.

17.4. Any communication for the purpose of direct marketing must contain:

17.4.1. Details of the identity of the sender; and

17.4.2. The address or other contact details to which the recipient may send a request to opt-out.

APPENDIX 1
REQUEST FOR INFORMATION FORM

1. PARTICULARS OF PERSON REQUESTING ACCESS TO INFORMATION			
Full Names & Surname:			
Identification Number:		**Cell phone no.**	
Other contact no:		**Fax no.**	
Email address:			
Postal address:		**Postal code**	
2. PARTICULARS OF PERSON ON WHOSE BEHALF THE REQUEST IS MADE			
*Only complete this section if a request for information is made on behalf of another person.			
Full Names & Surname/ Legal entity name:			
Identification/ Registration no.			
3. PARTICULARS OF REQUESTED INFORMATION			
*Provide full particulars of the information to which access is requested. If the Provided space is not sufficient, please continue on a separate page and attach it to the form. Any additional pages submitted must be signed.			
4. FORMAT IN WHICH INFORMATION IS REQUESTED			
*Indicate the format in which the information requested is required. Please note that the request for accessin the specified format may depend on the format in which the record is available and access in the requested format may be refused under certain circumstances.			
5. RIGHT TO BE EXERCISED OR PROTECTED			
*Indicate: 1. What right is to be exercised and/or protected and 2. Why the information is required to protect and/orto exercise this right.			
What right is to be protected			
Why the information is required			
6. NOTICE OF APPROVAL / REJECTION OF REQUEST			
Please note: You will be notified via e-mail and/or post whether your request has been approved or denied. If you wish to be informed in another manner, please specify the manner and provide the necessary details:			
7. PAYMENT DETAILS (Only applicable to Other Requesters)			
Kindly make payment of the amount of R_____ into the following bank account and attach proof of payment to this form.			
Details provided upon request.			
8. SIGNATURE			
Signed at:_____on this_____day of_____20____			
_____ Name of person submitting the request		_____ Signature of person submitting the request	