



PAIA & POPI MANUAL

Prepared in terms of Section 51 of the Promotion of Access to Information Act, No. 2 of 2000, (“PAIA”), and Section 18 of the Protection of Personal Information Act, No. 4 of 2013, (“POPI”).

CLACK & ASSOCIATES CC (“The Private Body”)

REGISTRATION NUMBER 1997/066856/23

TABLE OF CONTENTS

1. LIST OF ACRONYMS AND ABBREVIATIONS	3
2. PURPOSE OF PAIA MANUAL	3
3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF CLACK & ASSOCIATES CC	4
4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE	5
5. DESCRIPTION OF THE RECORDS OF CLACK & ASSOCIATES CC WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION	8
6. DESCRIPTION OF THE SUBJECTS ON WHICH THE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY CLACK & ASSOCIATES CC	9
7. PRESCRIBED FEES	10
8. PROTECTION OF PERSONAL INFORMATION	10
9. AVAILABILITY OF THE MANUAL	16
10. UPDATING OF THE MANUAL	17

1. LIST OF ACRONYMS AND ABBREVIATIONS

1.1	“CEO”	Chief Executive Officer
1.2	“DIO”	Deputy Information Officer;
1.3	“IO“	Information Officer;
1.4	“Minister”	Minister of Justice and Correctional Services;
1.5	“PAIA”	Promotion of Access to Information Act No. 2 of 2000(as Amended;
1.6	“POPIA”	Protection of Personal Information Act No.4 of 2013;
1.7	“Regulator”	Information Regulator; and
1.8	“Republic”	Republic of South Africa

2. PURPOSE OF PAIA MANUAL

This PAIA Manual is useful for the public to-

- 2.1 check the categories of records held by a body which are available without a person having to submit a formal PAIA request;
- 2.2 have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject;
- 2.3 know the description of the records of the body which are available in accordance with any other legislation;
- 2.4 access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;

- 2.5 know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;
- 2.6 know if the body will process personal information, the purpose of processing of personal information and the description of the categories of data subjects and of the information or categories of information relating thereto;
- 2.7 know the description of the categories of data subjects and of the information or categories of information relating thereto;
- 2.8 know the recipients or categories of recipients to whom the personal information may be supplied;
- 2.9 know if the body has planned to transfer or process personal information outside the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied; and
- 2.10 know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF CLACK & ASSOCIATES CC

3.1. Designated and Authorised Persons:

Directors: Etienne Clack
Daniel Clack

3.2. Chief Information Officer

Name: Etienne Clack
Tel: (083) 377 3301
Email: etienne@clack.co.za

3.3. Deputy Information Officer

Name: Daniel Clack
Tel: (078) 160 8470
Email: daniel@clack.co.za

3.4 Access to information general contacts

Email: admin@clack.co.za

3.5 Head Office

Postal Address: 78 Longlands Country Estate,
Polkadraai Road, Stellenbosch, 7600.

Physical Address: 78 Longlands Country Estate,
Polkadraai Road, Stellenbosch, 7600.

Telephone: (072) 695 8689

3.6 Email: admin@clack.co.za

3.7 Website: www.clack.co.za

4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

4.1. The Information Regulator ("IR"), in terms of section 10(1) of PAIA, must update and make available the revised Guide on how to use PAIA ("Guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

4.2. The contact details of the Information Regulator are:

4.2.1. Telephone: +27 10 023 5200

4.2.2. Telefax: +27 86 500 3351

4.2.3. Postal Address: PO Box 31533, Braamfontein, Johannesburg, 2017

4.2.4. Physical Address: JD House, 27 Stiemens Street, Braamfontein, Johannesburg,
2017

4.2.5. Website: <https://www.justice.gov.za/infoereg/>

4.2.6. Email: enquiries@infoeregulator.org.za

- 4.3. The South African Human Rights Commission (“the HRC”) has compiled a guide, in terms of section 10(1) of PAIA, containing information to assist any person who wishes to exercise any right as contemplated in PAIA.
- 4.4. The SAHRC Guide is available from the SAHRC. The contact details of the SAHRC are:
- 4.4.1. Telephone: +27 11 484 8300
 - 4.4.2. Telefax: +27 11 484 0582
 - 4.4.3. Postal address: Private Bag 2700, Houghton, 2041
 - 4.4.4. Website: www.sarhc.org.za
 - 4.4.5. Email: paia@sarhc.org.za
- 4.5. The aforesaid “Guide” contains the description of-
- 4.5.1. the objects of PAIA and POPIA;
 - 4.5.2. the postal and street address, phone and fax number and, if available, electronic mail address of-
 - 4.5.2.1. the Information Officer of every public body, and
 - 4.5.2.2. every Deputy Information Officer of every public and private body designated in terms of section 17(1) of PAIA¹ and section 56 of POPIA²;
 - 4.5.3. the manner and form of a request for-
 - 4.5.3.1. access to a record of a public body contemplated in section 11³; and

¹ Section 17(1) of PAIA- *For the purposes of PAIA, each public body must, subject to legislation governing the employment of personnel of the public body concerned, designate such number of persons as deputy information officers as are necessary to render the public body as accessible as reasonably possible for requesters of its records.*

² Section 56(a) of POPIA- *Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of POPIA.*

³ Section 11(1) of PAIA- *A requester must be given access to a record of a public body if that requester complies with all the procedural requirements in PAIA relating to a request for access to that record; and access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.*

- 4.5.3.2. access to a record of a private body contemplated in section 50⁴;
- 4.5.4. the assistance available from the IO of a public body in terms of PAIA and POPIA;
- 4.5.5. the assistance available from the Regulator in terms of PAIA and POPIA;
- 4.5.6. all remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging-
 - 4.5.6.1. an internal appeal;
 - 4.5.6.2. a complaint to the Regulator; and
 - 4.5.6.3. an application with a court against a decision by the information officer of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body;
- 4.5.7. the provisions of sections 14⁵ and 51⁶ requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;
- 4.5.8. the provisions of sections 15⁷ and 52⁸ providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

⁴ Section 50(1) of PAIA- A requester must be given access to any record of a private body if-

- a) that record is required for the exercise or protection of any rights;
- b) that person complies with the procedural requirements in PAIA relating to a request for access to that record; and
- c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

⁵ Section 14(1) of PAIA- The information officer of a public body must, in at least three official languages, make available a manual containing information listed in paragraph 4 above.

⁶ Section 51(1) of PAIA- The head of a private body must make available a manual containing the description of the information listed in paragraph 4 above.

⁷ Section 15(1) of PAIA- The information officer of a public body, must make available in the prescribed manner a description of the categories of records of the public body that are automatically available without a person having to request access

⁸ Section 52(1) of PAIA- The head of a private body may, on a voluntary basis, make available in the prescribed manner a description of the categories of records of the private body that are automatically available without a person having to request access

4.5.9. the notices issued in terms of sections 22⁹ and 54¹⁰ regarding fees to be paid in relation to requests for access; and

4.5.10. the regulations made in terms of section 92¹¹.

4.6. Members of the public can inspect or make copies of the Guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

5. DESCRIPTION OF THE RECORDS OF CLACK & ASSOCIATES CC WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

5.1 Promotion of Access to Information Act, No. 2 of 2000

5.2 Companies Act, No. 71 of 2008

5.3 Income Tax Act, No. 58 of 1962

5.4 Value Added Tax Act, No. 89 of 1991

5.5 Labour Relations Act, No. 66 of 1995

5.6 Basic Conditions of Employment Act, No. 75 of 1997

5.7 Employment Equity Act, No. 55 of 1998

5.8 Unemployment Insurance Act, No. 63 of 2001

5.9 Electronic Communications and Transactions Act, No. 25 of 2002

5.10 Financial Advisory and Intermediary Services Act, No. 37 of 2002

5.11 Close Corporations Act, No. 69 of 1984

5.12 Copyright Act, No. 98 of 1978

5.13 Long-Term Insurance Act, No. 52 of 1998

5.14 Any Other Industry Applicable Legislation

⁹ Section 22(1) of PAIA- The information officer of a public body to whom a request for access is made, must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

¹⁰ Section 54(1) of PAIA- The head of a private body to whom a request for access is made must by notice require the requester to pay the prescribed request fee (if any), before further processing the request.

¹¹ Section 92(1) of PAIA provides that –“The Minister may, by notice in the Gazette, make regulations regarding-

- (a) any matter which is required or permitted by this Act to be prescribed;
- (b) any matter relating to the fees contemplated in sections 22 and 54;
- (c) any notice required by this Act;
- (d) uniform criteria to be applied by the information officer of a public body when deciding which categories of records are to be made available in terms of section 15; and
- (e) any administrative or procedural matter necessary to give effect to the provisions of this Act.”

6. DESCRIPTION OF THE SUBJECTS ON WHICH THE BODY HOLDS RECORDS AND CATEGORIES OF RECORDS HELD ON EACH SUBJECT BY CLACK & ASSOCIATES CC

Subjects on which the body holds records	Categories of records
Financial	- Financial statements - Financial and tax records (company and employees) - Asset register - Management accounts
Human Resources	- HR policies and procedures - Advertised posts - Employees records - Codes of conduct - Internal policies applicable to employees
Internal Compliance and Administration	- Internal auditing and risk - Regulatory reports - Legislative compliance
Product Providers and Third Parties	- Contractual agreements - List of product providers - Any records a client has provided to the Private Body or a third party acting for or on behalf of the Private Body.
Client Records	- Any records a client has provided to the Private Body or a third party acting for or on behalf of the Private Body. - Contractual information - Personal records of clients - Client needs assessments - Client evaluation records - Client account numbers - Records generated by the Private Body pertaining to clients

Subjects on which the body holds records	Categories of records
Other	- Information technology including information systems, network security, software licenses and technology assets - Research information belonging to the Private Body - Internal communication - Market information - Support services

7. PRESCRIBED FEES

The following applies to requests (other than personal requests):

- 7.1 A requestor is required to pay the prescribed fees (R50.00) before a request will be processed;
- 7.2 If the preparation of the record requested requires more than the prescribed hours (six), a deposit shall be paid (of not more than one third of the access fee which would be payable if the request were granted);
- 7.3 A requestor may lodge an application with a court against the tender/payment of the request fee and/or deposit;
- 7.4 Records may be withheld until the fees have been paid.
- 7.5 The fee structure is available on the website of the SOUTH AFRICAN HUMAN RIGHTS COMMISSION at www.sahrc.org.za.

8. PROTECTION OF PERSONAL INFORMATION

8.1 Introduction

The right to privacy is an integral human right recognized and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA"). POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

Through the provision of quality goods and services, the FSP is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employee's and other stakeholders. A person's right to privacy

entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

Given the importance of privacy, the FSP is committed to effectively managing personal information in accordance with POPIA's provisions.

8.2 Policy Purpose

The purpose of this policy is to protect the FSP from the compliance risks associated with the protection of personal information which includes:

- Breaches of confidentiality. For instance, the FSP could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
- Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the FSP uses information relating to them.
- Reputational damage. For instance, the FSP could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the FSP.

We incorporate the requirements of data security, as dictated by the Act into all business processes. This policy aims to provide a guideline as to the processes and/or POPI related aspects that needs to be taken into consideration to attain data security and to protect personal information being gathered and stored, from unauthorized access and security breaches.

This policy demonstrates the FSP's commitment to protecting the privacy rights of data subjects in the following manner:

- Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
- By cultivating an organisational FSP culture that recognises privacy as a valuable human right.
- By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
- By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the FSP.
- By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the FSP and data subjects.

- By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

8.3 Policy Application

This policy and its guiding principles applies to:

- The FSP's governing body
- All branches, business units and divisions of the FSP
- All employees and volunteers
- All contractors, suppliers and other persons acting on behalf of the FSP

The policy's guiding principles find application in all situations and must be read in conjunction with POPIA as well as the FSP's PAIA Policy as required by the Promotion of Access to Information Act (Act No 2 of 2000).

The legal duty to comply with POPIA's provisions is activated in any situation where there is:

- processing of personal information, entered into a record by or for a responsible person, who is domiciled in South Africa.

POPIA does not apply in situations where the processing of personal information:

- is concluded during purely personal or household activities, or
- where the personal information has been de-identified.

8.4 Purpose of Processing Personal Information

The purpose or reasons for processing personal information in our organisation is to conduct a financial needs analysis on our clients.

8.5 Employees and other Persons acting on behalf of the FSP

Employees and other persons acting on behalf of the FSP will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees. Employees and other persons acting on behalf of the FSP are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.

Employees and other persons acting on behalf of the FSP may not directly or indirectly, utilise, disclose or make public in any manner to any person or third party,

either within the FSP or externally, any personal information, unless such information is already publicly known or the disclosure is necessary in order for the employee or person to perform his or her duties. Employees and other persons acting on behalf of the FSP must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.

Employees and other persons acting on behalf of the FSP will only process personal information where:

- The data subject, or a competent person where the data subject is a child, consents to the processing; or
- The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
- The processing complies with an obligation imposed by law on the responsible party; or
- The processing protects a legitimate interest of the data subject; or
- The processing is necessary for pursuing the legitimate interests of the organisation or of a third party to whom the information is supplied.

Furthermore, personal information will only be processed where the data subject:

- Clearly understands why and for what purpose his, her or its personal information is being collected; and
- Has granted the organisation with explicit written or verbally recorded consent to process his, her or its personal information.

Employees and other persons acting on behalf of the FSP will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.

Informed consent is therefore when the data subject clearly understands for what purpose his, her or its personal information is needed and who it will be shared with. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the FSP will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.

Consent to process a data subject's personal information will be obtained directly from the data subject, except where:

- the personal information has been made public, or
- where valid consent has been given to a third party, or
- the information is necessary for effective law enforcement.

Employees and other persons acting on behalf of the FSP will under no circumstances:

- Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks or duties.
- Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smart phones. All personal information must be accessed and updated from the organisation's central database or a dedicated server.
- Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
- Transfer personal information outside of South Africa without the express permission from the Information Officer. Employees and other persons acting on behalf of the organisation are responsible for:
 - Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
 - Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
 - Ensuring that personal information is encrypted (where possible) prior to sending or sharing the information electronically. The person responsible for the IT function will assist employees and where required, other persons acting on behalf of the FSP, with the sending or sharing of personal information to or with authorised external persons.
 - Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
 - Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.

- Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
- Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
- Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
- Undergoing POPI Awareness training from time to time. Where an employee, or a person acting on behalf of the FSP, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

8.6 Description of the categories of Data Subjects and of the information or categories of information relating thereto

Categories of Data Subjects	Personal Information that may be processed
Customers / Clients	Name, physical address, registration numbers or identity numbers, financial information, race, gender, sex, marital status, e-mail address, cellphone number, employment status and bank details.
Product or Service Providers	Names, registration number, vat numbers, address, trade secrets and bank details
Employees	Physical address, telephone number, identity number, education/qualifications, medical, gender and race.

8.7 The recipients or categories of recipients to whom the personal information may be supplied

Category of personal information	Recipients or Categories of Recipients to whom the personal information may be supplied
Identity number and names, for criminal checks	South African Police Services
Qualifications, for qualification verifications	South African Qualifications Authority
Credit and payment history, for credit information	Credit Bureaus

8.8 Planned transborder flows of personal information

None.

8.9 General description of Information Security Measures to be implemented by the responsible party to ensure the confidentiality, integrity and availability of the information

The nature of the security safeguards implemented or under implementation are to ensure the confidentiality and integrity of the personal information under the care of the body. This may, for example, include Data Encryption; Anti-virus and Anti-malware Solutions and Passwords Protections.

9. AVAILABILITY OF THE MANUAL

9.1 A copy of the Manual is available-

9.1.1 on www.clack.co.za;

9.1.2 head office of Clack & Associates CC for public inspection during normal business hours;

9.1.3 to any person upon request and upon the payment of a reasonable prescribed fee; and

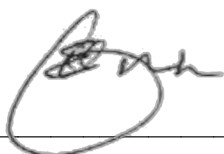
9.1.4 to the Information Regulator upon request.

9.2 A fee for a copy of the Manual, as contemplated in annexure B of the Regulations, shall be payable per each A4-size photocopy made.

10. UPDATING OF THE MANUAL

The head of Clack & Associates CC will on a regular basis update this manual.

Issued by



Etienne Clack

THE HEAD OF THE PRIVATE BODY