POPIA Compliance Office Manual

African Recovery Solutions

CONTENTS

CONTENTS 2
GLOSSARY 3
1. PURPOSE OF THIS POPIA COMPLIANCE OFFICE MANUAL 4
2. RECORDS OF PROCESSING ACTIVITIES – Company Procedure 4
2.1 Collecting Personal Information 4
2.2 Staff Responsibility 4
2.3 Client Consent 5
3. RECORDS OF PROCESSING ACTIVITIES – Section 51 PAIA Manual 5
a description of the categories of data subjects and of the categories of personal information; 5
3.1 Identifying the Responsible Party 6
3.2 Purpose of the Processing 6
3.3 Categories of Personal information 6
3.4 Justification for Processing Personal Information 6
3.5 Categories of Recipients to Whom Personal information may be disclosed 7
3.6 Transfers to a Third Country 8
3.7 Retention Periods 8
3.8 Security Measures 9
4. COMPLIANCE WITH THE CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION 10
4.1 Accountability 11
4.2 Processing limitation 12
4.3 Purpose Specification and Further Processing Limitation 13
4.4 Information quality 13
4.5 Openness 13
4.6 Security Safeguards 15
4.7 Data Subject Participation 16
5. COMPLIANCE WITH DATA SUBJECT RIGHTS 17
5.1. Right to be Informed 17
5.2. Right to Access 18
5.3. Right to Correction & Deletion 18
5.4. Right to Object 18
6. PERSONAL INFORMATION (SECURITY COMPROMISE) BREACH HANDLING 20
7. DATA PROTECTION IMPACT ASSESSMENT (DPIA) 22
8. INFORMATION OFFICERS (IO) 23
9. DATA PROTECTION AND CYBER SECURITY AWARENESS AND TRAINING DETAILS 24
10. EMPLOYEE/ OFFICE WORKERS CONFIDENTIALITY AGREEMENTS 25

GLOSSARY

The following definitions apply from section 1 of POPIA:

'Consent' of the data subject means any voluntary, specific and informed indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her;

'Responsible Party' means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

'**Personal information'** means any information relating to an identified or identifiable natural person ('data subject') or an existing juristic person; an identifiable natural person is one who can be identified, directly or indirectly. For example, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

'Personal information breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed;

'Processing' means any operation or set of operations which is performed on personal information or on sets of personal information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

'Operator' means a natural or legal person, public authority, agency or other body which processes personal information on behalf of the responsible party;

'Recipient' means a natural or legal person, public authority, agency or another body, to which the personal information are disclosed, whether a third party or not.

1. PURPOSE OF THIS POPIA COMPLIANCE OFFICE MANUAL

The Constitution of South Africa guarantees every individual the right to respect for his or her private and family life, home and communications, and the protection of their personal information. These rights have now been codified into regulations and national law. The Protection of Personal Information Act, 2013 (POPIA) came into force on the 1st July 2021.

The POPIA Act emphasises openness, security and accountability by responsible parties and operators, while at the same time standardising and strengthening the right of citizens to data privacy.

This document provides guidance as to how we could ensure that our Company is compliant with the POPIA Act.

This **Popia Compliance Office Handbook** focuses on **client personal information**, but is also applicable to all personal information processed by our Company, in all forms of media, including paper records, electronic records and documents, images, videos, SMS texts, online and electronic postings.

The law in this area is in evolution and we should refer to the website of www.assentcompliance.co.za for the latest version of the **Popia Compliance Office Handbook**. Please note that this **Popia Compliance Office Handbook** is for advice only and should not replace personalised legal advice.

2. RECORDS OF PROCESSING ACTIVITIES – Company Procedure

2.1 Collecting Personal Information

The Company's procedures for collecting personal information are set out below:

2.1.1 Company staff collect Clients / Third Party Contractors personal and demographic information via a service level agreement / application form. Clients are encouraged to pay attention to the collection statement that they complete as a new Client's / Third Party Contractor.

2.1.2 All Personal Information is acquired as a result of insurance claims received directly from our clients. This information is captured on the ARS system and is stored safely. Employees only have access to information on specific claims allocated to them.

2.2 Staff Responsibility

2.2.1 Comply with this handbook and the legislation applicable on the processing of personal information;

2.2.2 Collect personal information for the primary purpose of managing our relationship with our clients / third party contractors;

2.2.3 Take reasonable steps to make the client / third party contractor aware that our section 18 Privacy Notification is available at the office of the Information Officer.

2.3 Client Consent

2.3.1 The Company will only interpret and apply a client's / third party contractor consent for the primary purpose for which it was provided.

2.3.2 The Company staff must seek additional consent from the client's / third party contractor if the personal information collected may be used for any other purpose.

Form to be used:

Management Category	**Forms**
03_Data Subject Rights Policies & Procedure	03.2_Consent Form for Processing of Personal Information
	03.3_POPIA Section 18 Privacy Notification – Clients
07_Information Security Risk_Electronic Transmission	07.2_Client Consent for Electronic Communication

3. RECORDS OF PROCESSING ACTIVITIES – Section 51 PAIA Manual

Section 17 of POPIA specifies that each responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 51 of the Promotion of Access to Information Act, 2000 (PAIA). In terms of section 51 of PAIA this record must contain:

a) the name and contact details of the responsible party and, where applicable, the joint responsible party and the Company lead for data protection;

b) the purposes of the processing;

a description of the categories of data subjects and of the categories of personal information;

c) the categories of recipients to whom the personal information have been or will be disclosed;

d) where applicable, transfers of personal information to a third country;

e) the envisaged time limits for erasure of the different categories of data;

f) a general description of the technical and organisational security measures.

Form to be used:

Management Category	**Forms**
03_Data Subject Rights Policies & Procedure	*Form 03.19_Company Section 51 PAIA Manual*

It may assist in reviewing this document to consider the following issues:

3.1 Identifying the Responsible Party

If our Company is established as a legal entity, and determines the purpose of and means for processing personal information - our Company is the responsible party in processing personal information about our client's / third party contractor. Otherwise, we (and/or our colleagues if working in a group) should be identified as the responsible party or joint responsible parties. Employees are not responsible parties.

3.2 Purpose of the Processing

The data collected as part of the process of our service to clients will include a wide variety of **information all of which is necessary as part of the process of fulfilling our duties and** responsibilities as set out in the Service Level Agreement with our client's / third party contractor.

Purpose for processing personal information	
Client Personal Information	- retention of records as required by the law; - direct client's / third party contractor relations; - providing of services; - accessing products; - sharing with other third parties (with client consent and legal requirements); - collection of fees; - to manage our relationship with client's / third party contractor.

3.3 Categories of Personal information

3.3.1. Examples of the categories of data that might be collected include -

Administrative data which is necessary to support the administration of our Service Level Agreement e.g., name, address, contact details (phone, mobile, email), dates of engagement, etc.

Account Details which are required for providing a service and billing e.g.

a) The company name, surname and initials of the client's / third party contractor;

b) Contact particulars.

3.4 Justification for Processing Personal Information

3.4.1 The legal basis for processing of client's / third party contractor record data by our Company is provided by Section 11(1) in the POPIA Act – in respect of personal information.

3.4.2 Section 11(1) provides that Personal information may only be processed if -

(a) the data subject or a competent person where the data subject is a child consents to the processing;

(b) processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
(c) processing complies with an obligation imposed by law on the responsible party;
(d) processing protects a legitimate interest of the data subject;
(e) processing is necessary for the proper performance of a public law duty by a public body; or
(f) processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

Justification for processing personal information	
Client's / Third party contractor Personal Information	- Consent; - Conclusion or performance of a contract; - Obligation imposed by law; and - Pursuing our legitimate interests.

3.5 Categories of Recipients to Whom Personal information may be disclosed

3.5.1 These are broken down into four categories:

a) Sharing data in relation to the agreement between us and client / third party contractor;

b) Sharing data with data operators where a contract is required;

c) Sharing data under legal obligation;

d) Third Parties, with explicit client's / third party contractor consent.

Recipients with whom we may share personal information:

Categories of Recipient	Description
Agreement	Complete with categories of recipients you may share information with in terms of the agreement between you and the client's / third party contractor
Operators, with a contract	Company Software Vendors, Online Data Backup companies, Payroll Company; Billing Company
Legal Obligation	Employees personal information, for example SARS, UIF
Third Parties, with explicit Client's / Third Party Contractor consent	Attorneys, Insurance Companies, Companies, Banks

Form to be used:

Management Category	**Forms**
03_Data Subject Rights Policies & Procedure	*03.2_Consent to Process Personal Information*
	03.9_PAIA Form C_ Request for Access to Record of Private Body

3.6 Transfers to a Third Country

3.6.1 During standard operating procedures, client's / third party contractor records shall not be transferred outside of South Africa. Where client's / third party contractor data is to be transferred –

(a) explicit consent is required which must include informing the client's / third party contractor of the risks of such transfers of the personal information outside of the Republic;

(b) prior authorisation for transferring children's information from the Information Regulator is required – see the Guidance Note in ***Management Category 11_Legislation Regulations Ethical Handbook- 11.2.8_InfoRegSA-GuidanceNote-Processing-PersonalInformation-Children-20210628***

(c) prior authorisation for transferring special personal information from the Information Regulator is required – see the Guidance Note in Management Category 11_Legislation Regulations Ethical Handbooks - ***11.2.9_InfoRegSA-GuidanceNote-Processing-SpecialPersonalInformation-20210628 (1)***

3.7 Retention Periods

3.7.1 Personal information must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal information is processed.

3.7.2 The retention periods for records that can identify a living natural person or an existing juristic person are taken from various pieces of legislation.

Form to be used:

Management Category	**Forms**
00_Documentation Management	*00.2_Document Retention and Destruction Policy*
	00.4_Archiving of Records Register

	00.5_Record Disposal Certificate
	00.6_Records Disposal Register

3.8 Security Measures

3.8.1 We must commission regular information security audits to ensure that appropriate measures are in place to secure client's / third party contractor data in the Company. Such an audit should cover:

a) Operating Systems and Security Patches;
b) Hardware;
c) Networks, including Wi-Fi;
d) Anti-virus and anti-malware;
e) Firewalls;
f) Data Backup;
g) Access controls;
h) Appropriate use of the Internet.

Form to be used:

Management Category	**Forms**
00_Documentation Management	00.3_PI Assets Information Classification Guide
05_Create & Maintain Policies & Procedures	05.1_Information Quality Policy
	05.2_Minimum Access Policy
	05.3_Password Management Policy
	05.4_Acceptable Use Policy of Computer Equipment
	05.5_Social Media Policy
	05.6_Bring your Own Device Policy
	05.7_Clear Desk and Clear Screen Policy
	05.8_Shred-it All Policy
	05.10_Removable Media Policy
	05.11_Remote Working Policy
	05.12_ IT Equipment Disposal Policy

4. COMPLIANCE WITH THE CONDITIONS FOR THE LAWFUL PROCESSING OF PERSONAL INFORMATION

Our Company must ensure all personal information is processed in line with the 8 Conditions for the Lawful Processing of Personal Information in terms of POPIA and good practices. These conditions are:

8 Conditions for the Lawful Processing of Personal Information		
Condition 1	**Accountability**	
Condition 2	**Processing limitation**	Lawfulness of processing
		Minimality
		Consent, justification and objection
		Collection directly from data subject
Condition 3	**Purpose specification**	Collection for specific purpose
		Retention and restriction of records
Condition 4	**Further processing limitation**	Further processing to be compatible with purpose of collection
Condition 5	**Information quality**	Quality of information
Condition 6	**Openness**	Documentation
		Notification to data subject when collecting personal information
Condition 7	**Security Safeguards**	Security measures on integrity and confidentiality of personal information
		Information processed by operator or person acting under authority
		Security measures regarding information processed by operator
		Notification of security compromises
Condition 8	**Data subject participation**	Access to personal information
		Correction of personal information
		Manner of access

4.1 Accountability

In order to be accountable under the POPIA Act, there is a requirement on us to keep certain records. These include:

- Regular Information Security Audits;
- Records of Processing Activities – our **Form 03.19_Company Section 51 PAIA Manual**;
- Confidentiality agreements with Staff – our **Form 02.5_Access and Confidentiality Agreement with Employees**;
- Records of staff training and awareness – our **Form 06.1_Employee Training Log**;
- Operator contracts with Company Software Vendors and any other operators – our **Forms 08.2_Cover Letter Operator POPIA Compliance and 08.5_ Data Protection Agreement for Operators**;
- Where processing on basis of consent, records of this consent;

A member of staff should be appointed to a lead role on personal information protection and should be available to clients / third party contractors to discuss any personal information protection questions and to facilitate access requests for records.

Our responsibilities include -

(a) Accept responsibility to comply with the responsibilities under POPIA - see letter in ***Management Category 01.4_POPIA_Executive_Support_Letter***;

(b) Approve suitable policies and systems for the management and processing of personal information see policies in ***Management Category 05_Create & Maintain Policies & Procedures***;

(c) Ensure that policies and systems are understood, embraced and complied with – see training material in ***Management Category 06_Implement & Maintain Training & Awareness Program***;

(d) Ensure that staff members are properly equipped and trained to comply with POPIA – see training material in ***Management Category 06_Implement & Maintain Training & Awareness Program***;

(e) Ensure that contracts with employees third parties capture relevant POPIA responsibilities - see letter in ***Management Category 08_Managing Third Party Compliance - 08.2_Letter Operator POPIA Compliance***; and

(f) Regularly monitor and review the effectiveness of policies and systems.

Form to be used:

Management Category	**Forms**
01_Preparation for the Project	01.4_POPIA_Executive_Support_Letter
05_Create & Maintain Policies & Procedures	All policies

06_Implement & Maintain Training & Awareness Program	All policies
08_Managing Third Party Compliance	All policies

4.2 Processing limitation

4.2.1 We must ensure personal information is processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

4.2.2 In essence, there must be a legal basis for the processing of personal information of any data subject.

4.2.3 The purpose for processing personal information must be:

(a) Adequate

(b) Relevant

(c) Not Excessive

4.2.4 Section 2 of this Handbook describes Records of Processing Activities detailing the lawfulness of processing of personal information, purpose of processing, lawfulness of processing, categories of recipients to whom the personal information will be disclosed, and envisaged time period for retention. Any processing activities outside of the areas detailed in Section 2 require us to document the processing activity extensions in a similar form to Section 2.

4.2.5 Personal information must be collected directly from the data subject, except if—

a) the information is contained in or derived from a public record or has deliberately been made public by the data subject;

b) the data subject or a competent person where the data subject is a child has consented to the collection of the information from another source;

c) collection of the information from another source would not prejudice a legitimate interest of the data subject; collection of the information from another source is necessary—

(i) to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

(ii) to comply with an obligation imposed by law or to enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act, 1997 (Act No. 34 of 1997);

(iii) for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

(v) to maintain the legitimate interests of the responsible party or of a third party to whom the information is supplied;

(e) compliance would prejudice a lawful purpose of the collection; or

(f) compliance is not reasonably practicable in the circumstances of the particular case.

4.3 Purpose Specification and Further Processing Limitation

We are only permitted to collect and process information for an explicit purpose. If our Company is carrying out any additional processing beyond what is normal practice, then it must be included in our Record of Processing Activities as defined in Section 2 of this Handbook. There must also be a legal basis for such additional processing and it must be transparent to the client / third party contractor.

4.4 Information quality

4.4.1 Personal information shall be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal information which is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay.

4.4.2 We must take all reasonable efforts to ensure the accuracy of the client / third party contractor data. For example, if a client / third party contractor has moved office, a record showing that he is currently living at his old address is obviously inaccurate. But a record showing his former address remains accurate, even though he no longer lives there.

4.4.3 However, we may legitimately wish to retain a record of our opinion. It is acceptable to keep records of events that may have happened in error, provided those records are not misleading about the facts.

Form to be used:

Management Category	**Forms**
05_Create & Maintain Policies & Procedures	05.1_Information Quality Policy

4.5 Openness

4.5.1 We must maintain the documentation of all processing operations under our responsibility as referred to in section 51 of the Promotion of Access to Information Act.

4.5.2 In addition, a Company section 18 Privacy Notification should provide details to the data subject in a concise, transparent, intelligible and easily accessible form including:

a) The identity and contact details of the responsible party;

b) The identity of the staff member with responsibility for data protection;

c) What information is being collected;

d) Purposes of processing;

e) Recipients or categories of recipients with whom their personal information will be disclosed;

f) Period of processing;

g) Their rights;

h) Lawful basis for the processing

4.5.3 The **Company privacy statement** must be made available to data subjects when they register with us.

4.5.4 The primary processing of client / third party contractor personal information in our Company is necessary in order to deliver a service. The lawfulness of such processing is defined in Section 2 (lawfulness of processing) and is generally not based on consent.

4.5.5 However, there are specific processing conditions where consent is required, particularly when disclosing of special personal information to recipients. We must be able to demonstrate that the data subject has consented to this processing, and this consent must be informed, freely given, and provided in a clear and transparent manner. Specifically, where the lawfulness of processing requires explicit consent, there shall be procedures for collecting this consent. We must also monitor all requests for removal or withdrawals of consent, document such requests in the client / third party contractor record and ensure that all removals are completed within undue delay - **see *Management Category 03_Data Subject Rights Policies & Procedure 03.2_Authorisation for Release of Personal Information to Third Parties***.

4.5.6 Overall, data processing must be open and transparent and the client / third party contractor should not be surprised by any disclosures outside of our Company.

4.5.7 Section 17 of POPIA stipulates that a responsible party must maintain the documentation of all processing operations under its responsibility as referred to in section 51 of the Promotion of Access to Information Act, 2000 (PAIA) – **see form 03.19_Company Section 51 PAIA Manual.**

4.5.8 All requests for personal information and records from any person or entity (attorneys, insurance companies, employers, etc.) shall be dealt with in accordance with the Company section 51 PAIA manual by using **form 03.9_PAIA Form C_ Request for Access to Record of Private Body.**

Form to be used:

Management Category	**Forms**

03_Data Subject Rights Policies & Procedure	*03.3_POPIA Section 18 Privacy Notification – Clients*
	Procedure 03.2_Consent to Process Personal Information
	Form 03.19_Company Section 51 PAIA Manual
	Form 03.9_PAIA Form C_ Request for Access to Record of Private Body

4.6 Security Safeguards

4.6.1 We must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

4.6.2 What does Security measures on integrity and confidentiality of personal information mean in the Company?

a) The Company must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent –

(i) loss of, damage to or unauthorised destruction of personal information; and

(ii) unlawful access to or processing of personal information.

b) In order to give effect to that, we must take reasonable measures to -

(i) identify all reasonably foreseeable internal and external risks to personal information in our possession or under our control;

(ii) establish and maintain appropriate safeguards against the risks identified;

(iii) regularly verify that the safeguards are effectively implemented; and

(iv) ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

4.6.3 The Company must have due regard to generally accepted information security organisations and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

4.6.4 We must commission regular information security audits to ensure that appropriate measures are in place to secure client / third party contractor data in the Company. The audit should cover both technical and organisational aspects of information security.

see Management Category 05_Create & Maintain Policies & Procedures.

Form to be used:

Management Category	**Forms**
05_Create & Maintain Policies & Procedures	*05.1_ Information Quality Policy*
	05.2_Minimun Access Policy
	05.3_Password Management Policy
	05.4_ Acceptable Use Policy of Computer Equipment
	05.5_Social Media Policy
	05.6_Bring your Own Device Policy
	05.7_Clear Desk and Clear Screen Policy
	05.8_Shred-it All Policy
	05.10_Removable Media Policy

4.7 Data Subject Participation

See Section 5 hereunder.

Form to be used:

Management Category	**Forms**
03_Data Subject Rights Policies & Procedure	*03.2_Consent to Process Personal Information*
	03.3_POPIA Section 18 Privacy Notification – client / third party contractor
07_Information Security Risk_Electronic Transmission	07.2_Client Consent for Electronic Communication

5. COMPLIANCE WITH DATA SUBJECT RIGHTS

Client / Third Party Contractors personal information belongs to the individual or juristic person, and they have a number of rights to their personal information. We must have procedures in place in the Company to support the individual rights discussed below.

It is important for us to verify the identity of a Client / Third Party Contractor making a data subject request in order to ensure the personal information is only provided to the data subject

5.1. Right to be Informed

5.1.1. What is the right to be informed and why is it important?

a) The POPIA Act provides that a data subject has the right to be notified that -

b) personal information about him, her or it is being collected (Section 18 Privacy Notification) - **see *Management Category 03_Data Subject Rights Policies & Procedure – Form 03.3_POPIA Section 18 Privacy Notification - Client / Third Party Contractor***; or

c) his, her or its personal information has been accessed or acquired by an unauthorised person **see *Management Category 10_Implement & Maintain Security Incident Procedures – Form 10.3_Data Breach_Security Compromise Report Form***

d) Getting this wrong can leave us open to fines, lead to reputational damage and possible disciplinary steps against employees.

Forms to be used:

Management Category	**Forms**
03_Data Subject Rights Policies & Procedure	*03.3_POPIA Section 18 Privacy Notification – Client / Third Party Contractor*
10_Implement & Maintain Security Incident Procedures	*Form 10.2_Data Breach_Security Compromise Report Form*

5.1.2. When should we provide privacy information?

a) When we collect personal information directly from the Client / Third Party Contractor it relates to, we must provide them with a privacy notification before the information is collected, unless the data subject is already aware of the information.

b) In any other case, before the information is collected or as soon as reasonably practicable after it has been collected.

Form to be used:

Management Category	**Forms**

03_Data Subject Rights Policies & Procedure	*03.3_POPIA Section 18 Privacy Notification - Client / Third Party Contractor*

5.2. Right to Access

5.2.1. The Promotion of Access to Information Act 2000 gives everyone the right of access to records held by either public or private bodies for legitimate purposes. In the latter case, people should be allowed access to "any information that is held by another person and that is required for the exercise or protection of any rights".

5.2.2. Either the Client / Third Party Contractor him/herself, or someone authorised to act on the Client / Third Party Contractor's behalf, can request access; ordinarily the request itself is made in writing and should be responded to within 30 calendar days.

Form to be used:

Management Category	**Forms**
03_Data Subject Rights Policies & Procedure	*03.2_Consent to Process Personal Information*
	03.9_PAIA Form C_ Request for Access to Record of Private Body
	03.6_Data Subject Request Register

5.3. Right to Correction & Deletion

a) The Client / Third Party Contractor has the right to obtain correction of records which are factually inaccurate. However, this is not an unqualified right and depends on the circumstances of each case.

b) POPIA also deals with the right to deletion. This would need to be examined on a case-by-case basis and it might be appropriate to seek independent legal advice or the opinion of our indemnifiers. We should keep a record of this advice.

Form to be used:

Management Category	**Forms**
03_Data Subject Rights Policies & Procedure	*03.8_Request Correction Deletion Personal Information*
	03.6_Data Subject Request Register

5.4. Right to Object

a) Individuals have a right to object at any time to processing of personal information for direct marketing purposes, in which case the personal information shall no longer be

processed for such purposes. Other objections must be dealt with on a case-by-case basis.

Form to be used:

Management Category	**Forms**
03_Data Subject Rights Policies & Procedure	*03.7_Objection to the Processing of Personal Information*
	03.6_Data Subject Request Register

6. PERSONAL INFORMATION (SECURITY COMPROMISE) BREACH HANDLING

6.1. "Personal Security Compromise" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal information transmitted, stored or otherwise processed.

6.2. Example of typical Data Breaches are:

a) Loss or theft of personal information or equipment on which personal information is stored;

b) Loss or theft of documents/folders;

c) Unforeseen circumstances such as a flood or fire which destroys information;

d) Inappropriate access controls allowing unauthorised use;

e) A hacking/cyber-attack (such as ransomware);

f) Obtaining information from the Company by deception;

g) Misaddressing of e-mails/human error.

6.3. Notifying the Information Regulator

6.3.1. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the responsible party must notify -

(a) the Regulator; and

(b) subject to subsection (3), the data subject, unless the identity of such data subject cannot be established.

6.3.2. The notification must be made as soon as reasonably possible after the discovery of the compromise, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of the responsible party's information system.

6.3.3. The responsible party may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

6.4. Notifying Data Subjects

6.4.1. The notification to a data subject must be in writing and communicated to the data subject in at least one of the following ways:

a) Mailed to the data subject's last known physical or postal address;

b) sent by e-mail to the data subject's last known e-mail address;

c) placed in a prominent position on the website of the responsible party;
d) published in the news media; or
e) as may be directed by the Regulator.

6.4.2 The notification referred to in subsection (1) must provide sufficient information to allow the data subject to take protective measures against the potential consequences of the compromise, including -

a) a description of the possible consequences of the security compromise;
b) a description of the measures that the responsible party intends to take or has taken to address the security compromise;
c) a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
d) if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

6.4.3. The Regulator may direct a responsible party to publicise, in any manner specified, the fact of any compromise to the integrity or confidentiality of persona

Form to be used:

Management Category	**Forms**
10_Implement & Maintain Security Incident Procedures	*10.1_Data Breach Policy_Security Compromise Policy*
	10.2_Data Breach_Security Compromise Report Form
	10.3. Breach Risk Assessment

7. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Data Protection Impact Assessments (DPIAs) (Risk Assessment) is a method of assessing the level of data protection in place to safeguard clients' / third party contractors' personal information. They are a useful learning process for companies and are helpful in identifying risk. DPIAs are important tools for ensuring good practice and accountability, as they help responsible parties not only to comply with requirements of the POPIA, but also to demonstrate that appropriate actions have been taken to ensure the correct measures are in place to protect the privacy of individuals. Mandatory in terms of paragraph 4(1)(b) of the Regulations in terms of the POPIA Act.

Form to be used:

Management Category	**Forms**
01_Preparation for the Project	*01.2_POPIA Personal Information Protection Assessment.*

8. INFORMATION OFFICERS (IO)

Information Officers are, by virtue of their positions, appointed automatically in terms of PAIA and POPIA. The following are categories of Information Officers per specific Body –

Private Body	*Natural Person*	*Sole proprietor who carries on any trade, business or profession, but only in such capacity and not in his personal capacity*
	Partnership	*Any partner of the partnership or any person duly authorised by the partnership.*
	Juristic Person	*Chief Executive Officer or the Managing Director or equivalent officer of the juristic person or any person duly authorised by that officer or any person who is acting as such or any person duly authorised by such acting person.*

Our Information officer will need to register with the Information Regulator. The portal for registration is unavailable at the moment. On the 22nd June 2021 the Information Regulator released a notice saying that



Form to be used:

Management Category	**Forms**
02_Implement & Maintain Governance & Leadership Structure	*02.2_Registration Information Officer*
	02.3_Authorisation Letter Information Officer
	02.4_Designation Letter Deputy Information Officer

Guidelines:

Management Category	**Forms**
11.2_Information Regulator	*11.2.7_InfoRegSA-GuidanceNote-IO-DIO-20210401*

9. DATA PROTECTION AND CYBER SECURITY AWARENESS AND TRAINING DETAILS

All staff members need regular training in data protection and cyber security. A log of training activities should be maintained. Signed confirmation of training completed per employee should be retained. Assent Compliance (https://assentcompliance.co.za/) is exploring the possibility of providing access to suitable online training for Company staff.

Form to be used:

Management Category	**Forms**
06_Implement & Maintain Training & Awareness Program	*06.1_Employee Training Log*
	06.2_Employee Training Programme
	POPIA Awareness1_An Overview_Leadership
	POPIA Awareness2_An Overview_All Staff
	POPIA Awareness3_Mobile Devices_All Staff
	POPIA Awareness4_Security Measures - Leadership
	POPIA Awareness5_Collection of Personal Information - All Staff
	POPIA Awareness6_Data Subject Rights - All Staff
	Poster - Compliance Awareness
	Poster - Email Phishing
	Poster - Insider, Accidental or Intentional Data Loss
	Poster - Legal basis for processing personal information
	Poster - Loss or Theft of Equipment and Data
	Poster - Make secure choices
	Poster - What is my responsibility regarding e-mail security
	Poster - What is my responsibility regarding passwords
	Poster - What is our client's (data subject) rights
	Poster - What is Personal Information
	Poster - What to do when Using a Mobile Device

10. EMPLOYEE/ OFFICE WORKERS CONFIDENTIALITY AGREEMENTS

Company support staff, such as managers, secretaries, receptionists and other employees must sign confidentiality agreements as part of their contract of employment. All staff joining and leaving the Company should be logged. Staff leaving the Company should have their access revoked, both to local and online applications and services, including backup services.

Form to be used:

Management Category	**Forms**
02_Implement & Maintain Governance & Leadership Structure	*02.5_Access and Confidentiality Agreement with Employees*
	02.6_Letter to Employees Privacy Notification
	02.7_POPIA Section 18 Privacy Notification - Employees