PICARO 107 CC t/a ALBAROSA GUEST HOUSE

2007/194156/23

Manual to give effect to the:

Promotion of Access to Information Act, 2000; and

Protection of Personal Information Act, 2013

30 June 2021

TABLE OF CONTENTS

[1] See Government Notice No. R.1383 of 14 December 2018 (Government Gazette No. 42110 of 14 December 2018) for a complete set of prescribed forms

PART ONE
PREAMBLE AND INTRODUCTION TO ACCESS TO INFORMATION AND PROTECTION OF PERSONAL INFORMATION

This document was prepared in accordance with the Promotion of Access to Information Act, 2000 and to address the requirements of the Protection of Personal Information Act, 2013.

The Bill of Rights in Section 32 of the Constitution of the Republic of South Africa, 1996 provides that everyone has the right of access to any information held by the State and any other person that is required for the exercise or protection of any rights. The Promotion of Access to Information Act, 2000 (hereinafter referred to as PAIA) gives effect to the such right.

The Bill of Rights in Section 14 of the Constitution provides that everyone has the right to privacy including a right to protection against the unlawful collection, retention, dissemination and use of personal information and that the State must respect, protect, promote and fulfil such rights. The Protection of Personal Information Act, 2013 (hereinafter referred to as POPIA) has been assented to by the Parliament to give effect to such rights.

This document must be read in conjunction with PAIA and POPIA and any Regulations promulgated in terms thereof. Where appropriate, references to specific provisions of both Acts are included as footnotes.

PART TWO
MANUAL IN TERMS OF THE PROMOTION OF ACCESS TO INFORMATION ACT, 2000

1. AVAILABILITY OF THIS MANUAL

This Manual[2] is available:

(a) On the website, if any, of the private body.
(b) At the principal place of business of the private body for public inspection during normal working hours.
(c) To any person upon request and upon the payment of R500.00 excluding VAT which is considered to be a reasonable amount having regard to time and expenses, unless a different fee is determined by the Information Regulator.[3]
(d) To the Information Regulator upon request.

2. NATURE OF THE PRIVATE BODY'S BUSINESS

Picaro 107 CC was established in terms of the Close Corporations Act, 1984 (No. 69 of 1984) and operates an accommodation facility (Albarosa Guest House).

3. PARTICULARS OF THE HEAD/INFORMATION OFFICER OF THE PRIVATE BODY

[2] Compiled in terms of section 51 of PAIA
[3] Regulation 4(2) of the Regulations relating to the Protection of Personal Information (Government Notice No.R.1383 of 14 December 2018)

The Head of the private body must, in addition to the duties and responsibilities referred to in Part Three, paragraph 11 of this Manual, ensure compliance with PAIA in so far as requests for access to records of the private body is concerned.[4]

The personal details of the Head /Information Officer of the private body are as follows:

Name: GS Moolman
Physical address: 7 Helderberg Street, Stellenbosch 7600
Cellphone number: 0837215786
E-mail address: info@albarosa.co.za
Website: www.albarosa.co.za

4. GUIDE ON HOW TO USE PAIA

The Information Regulator shall in accordance with section 10 of PAIA update and make available the existing guide that has been compiled by the South African Human Rights Commission containing such information, in an easily comprehensible form and manner, as may be reasonably required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

Enquiries in this regard must be directed to the Information Regulator at JD House, 27 Stiemens Street, Braamfontein, Johannesburg 2001, or PO Box 31533, Braamfontein, Johannesburg 2017, or email inforeg@justice.gov.za, or telephone number 012 315 1111, or by visiting the Information Regulator's website https://justice.gov.za/inforeg/

5. AUTOMATICALLY AVAILABLE RECORDS AND ACCESS THERETO

The Head of the private body may be consulted on the categories of records that are automatically available (if any) without a person having to formally request access thereto.[5]

Such categories shall include records that are already in the public domain and available:

(a) For inspection in terms of legislation other than PAIA.
(b) For purchase or copying from the private body.
(c) From the private body free of charge.

The Head of the private body may delete any part of a record contemplated above which, on a request for access, may or must be refused in accordance with the grounds for refusal of access to records.[6]

The only fee payable, if any, for access to a record that are automatically available shall be a prescribed fee for reproduction.

6. PROCEDURE FOR THE SUBMISSION OF A FORMAL REQUEST FOR ACCESS TO RECORDS AND FEES PAYABLE

Procedure for the submission of requests[7]

[4] Part 3 of PAIA
[5] Section 52 of PAIA
[6] Part 3, Chapter 4 of PAIA

Any request for access to a record of the private body must substantially correspond with the format of the prescribed application form for private bodies as contained in Regulation No.R.187 dated 15 February 2002 (form attached).

Such application must be directed to the Head of the private body at the address, email address or fax number as indicated in this Manual.

The requester must specify his/her email and postal address or fax number in the Republic of South Africa and indicate which applicable form of access is required.

Sufficient particulars must be provided to enable the Head of the private body to identify the requester, as well as the record or records requested.

The requester must identify the right he/she is seeking to exercise or protect and provide an explanation of why the requested record is required for the exercise or protection of that right.

If a request is made on behalf of a person, proof to the reasonable satisfaction of the Head of the private body must be submitted of the capacity in which the requester is making the request.

A requester shall within thirty (30) days, or such prescribed extended period[8], be notified by the Head of the private body whether a request for access to a record has been granted or refused[9] with due regard to the grounds for refusal of access to records.[10] If the requester in addition to a written reply wishes to be informed of the decision of the Head of the private body in any other manner, such manner and the necessary particulars to be so informed, must be stated.

The submission of a request for access to a record and any communication in that regard must not be construed that such request shall necessarily be granted by the Head of the private body.

Representations and complaints

A requester aggrieved by a decision of the Head of the private body to refuse a request for access or taken in terms of section 54, 57(1) or 60 of PAIA, or a third party aggrieved by a decision of the Head of the private body in relation to a request for access to a record of that body, may within 180 days of the decision submit a complaint alleging that the decision was not in compliance with PAIA, to the Information Regulator in the prescribed manner and form for appropriate relief.

Fees payable[11]

The Head of the private body shall by written notice require from any requester for access to a record to pay the prescribed request and appropriate access fees, if any, before the request is further processed.

---

[7] Section 53 of PAIA
[8] Section 57 of PAIA
[9] Section 56 of PAIA
[10] Chapter 4 of PAIA
[11] Section 54 of PAIA

The fee structure for the purpose of calculating the fees payable with regard to a request for access to a record of a private body, is prescribed by Regulation No.R.187 dated 15 February 2002 (fees attached). Such fee structure may from time to time be amended.

A requester who requests personal information about that requester is not liable for the payment of any fees in respect of such request.

A requester whose request for access to a record has been granted by the Head of the private body, must pay the prescribed access fee for reproduction, search and preparation of the record; provided that if in the opinion of the Head of the private body the time for search and preparation of the record will be in excess of six (6) hours, it shall be required from the requester to pay one third of the prescribed access fee as a deposit.

The Head of the private body shall withhold a record until the requester concerned has paid the applicable fees.

7. DESCRIPTION OF THE SUBJECTS ON WHICH THE PRIVATE BODY HOLD RECORDS AND CATEGORIES ON EACH SUBJECT[12]

Administrative records
Agreements/contracts (service providers, customers, etc.)
CC Registration Certificate
Customer records
Directors' details/shares
Licenses
Notices and minutes of meetings/resolutions
Records relating to the appointment of auditors/accountants/insurance brokers
Written communications/correspondence/reports

Personnel records
Attendance register
Casualty records
Disciplinary code/records
Employment contracts
Leave records
Procedural/training manuals/records
Remuneration records
UIF records

Financial records
Accounting records
Annual financial statements
Audit reports
Bank statements
Debtor/Creditor accounts
Guarantees
Income Tax/PAYE/VAT records
Income/expenditure budgets/statements
Insurance records

[12] Section 51(1)(b)(iv)

Invoices, receipts and claims

Records regarding movable and immovable property
Assets and liabilities
Inventory and stock in trade
Title Deed

8. DESCRIPTION OF RECORDS WHICH ARE AVAILABLE IN ACCORDANCE WITH ANY OTHER LEGISLATION

The private body may hold records in accordance with other legislation, such as the following, but not necessarily limited thereto:

Basic Conditions of Employment Act, 1997 (No. 75 of 1997)
Close Corporations Act, 1984 (No. 69 of 1984)
Compensation for Occupational Injuries and Health Diseases Act, 1993 (No. 103 of 1993)
Consumer Protection Act, 2008 (No. 68 of 2008)
Credit Agreements Act, 1980 (No. 75 of 1980)
Debt Collectors Act, 1998 (No. 114 of 1998)
Electronic Communication and Transaction Act, 2000 (No. 25 of 2002)
Employment Equity Act, 1998 (No. 55 of 1998)
Financial Intelligence Centre Act, 2001 (No. 38 of 2001)
Income Tax Act, 1967 (No.95 of 1967)
Labour Relations Act, 1995 (No. 66 of 1995)
Medical Schemes Act, 1998 (No. 131 of 1998)
National Credit Act, 2005 (No. 34 of 2005)
Occupational Health and Safety Act, 1993 (No. 85 of 1993)
Pension Funds Act, 1956 (No. 24 of 1956)
Tax Administration Act, 2011 (No. 28 of 2011)
Unemployment Insurance Act, 1966 (No. 30 of 1966)
Value Added Tax Act, 1991 (No. 89 of 1991)
Western Cape Land Use Planning Act, 2014 (No. 3 of 2014)/Land Use Planning Ordinance. 1985 (No. 15 of 1985)/municipal by-laws on land use planning
Western Cape Liquor Act, 2008 (No. 4 of 2008)

PART THREE
POLICY MANUAL IN TERMS OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013

1. POLICY STATEMENT

The private body is obliged in terms of the Protection of Personal Information Act, 2013 (POPIA) to, amongst others, operate good policies, procedures and practices to protect personal information.[13]

This Policy Manual is established to give effect to and facilitate compliance with POPIA.
Given the importance of privacy as recognized by the Constitution and international law, the private body is committed to effectively managing personal information in accordance with POPIA

[13] Section 109(3)(g) POPIA

read with other appropriate legislation such as the Promotion of Access to Information Act, 2000 (PAIA) and the Electronic Communications and Transactions Act, 2002.

2. PURPOSE OF THIS POLICY MANUAL

The purpose of this Policy Manual is to establish sustainable procedures and practices to process personal information and protecting the privacy rights of data subjects as follows:

(a) Through encouraging desired behaviour amongst its members and directing compliance with the provisions of POPIA and related legislation.
(b) By cultivating a culture amongst its members that recognises privacy as a valuable human right.
(c) By developing and implementing internal controls for the purpose of managing the compliance risks associated with the protection of personal information.
(d) By establishing sound measures that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the private body.
(e) By acknowledging the prescribed duties and responsibilities of, and assigning specific powers and duties to, the Information Officer in order to protect the interests of the private body and data subjects.
(f) By providing guidance, coaching and training appropriate to the extent and structure of the private body's business operations to members who process personal information on behalf of the private body so that they can act confidently and consistently.

3. APPLICATION OF THIS POLICY MANUAL

This Policy Manual applies to:

(a) The members of the private body/responsible party.
(b) Any branches, business units and divisions of the private body.
(c) Any operators and other persons authorised to act on behalf of the private body in relation to the processing of personal information.

This Policy Manual does not apply to the processing of personal information:[14]

(a) In the course of a purely personal or household activity.
(b) That has been de-identified to the extent that it cannot be re-identified again.
(c) By or on behalf of a public body in certain cases.

4. PURPOSE OF POPIA

The purpose of POPIA is to:[15]

(a) Give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party, subject to justifiable limitations that are aimed at balancing the right to privacy against other rights and protecting important interests, including the free flow of information within the Republic of South Africa and across international borders.

[14] Section 6 of POPIA
[15] Section 2 of POPIA

(b) Regulate the manner in which personal information may be processed by establishing conditions that prescribe the minimum threshold requirements for the lawful processing of personal information.
(c) Provide persons with rights and remedies to protect their personal information from unlawful processing.
(d) Establish voluntary and compulsory measures, including the establishment of an Information Regulator to ensure respect for and to promote, enforce and fulfil the rights protected by POPIA.

5. DEFINITIONS

For convenience, the following POPIA definitions are highlighted:[16]

Biometrics means a technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.

Child means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him/herself.

Competent person means any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.

Consent means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.

Data subject means the person to whom personal information relates.

De-identify in relation to personal information of a data subject, means to delete any information that identifies the data subject, or which can be used or manipulated by a reasonably foreseeable method to identify the data subject, or can be linked by a reasonably foreseeable method to other information that identifies the data subject; **de-identified** has a corresponding meaning.

Direct marketing means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of (a) promoting or offering to supply in the ordinary course of business any goods or services to the data subject, or (b) requesting the data subject to make a donation of any kind for any reason.

Electronic communication means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Filing system means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

Operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

[16] See section 1 of POPIA for the full text

Person means a natural person or juristic person.

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:

(a) 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.
(b) Information relating to the education or the medical, financial, criminal or employment history of the person.
(c) Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person.
(d) The biometric information of the person.
(e) The personal opinions, views or preferences of the person.
(f) 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.
(g) The views or opinions of another individual about the person.
(h) 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 revel information about the person.

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

(a) The collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use.
(b) Dissemination by means of transmission, distribution or making available in any other form.
(c) Merging, linking, as well as restriction, degradation, erasure or destruction of information.

Re-identify in relation to personal information of a data subject, means to resurrect any information that has been de-identified, that:

(a) Identifies the data subject.
(b) Can be used or manipulated by a reasonably foreseeable method to identify the data subject, or
(c) Can be linked by a reasonably foreseeable method to other information that identifies the data subject; and **re-identified** has a corresponding meaning.

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.

Restriction means to withhold from circulation, use or publication any personal information that forms part of a filing system, but not to delete or destroy such information.

Special personal information means personal information as referred to in section 26 of POPIA.

Unique identifier means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

6. RIGHTS OF DATA SUBJECTS

The private body recognises that a data subject has the right to have his/her personal information processed in accordance with the conditions for the lawful processing of personal information as contemplated in POPIA[17].

The responsible party and other persons authorized to act on behalf of the private body shall exercise such lawfully established rights diligently, including but not limited to the following:[18]

6.1 The right to be notified

A data subject shall be notified that personal information about him/her is being collected or that his/her personal information has been accessed or acquired by an unauthorised person.

6.2 The right to access personal information

A data subject may at any time establish whether the responsible party holds personal information related to him/her and to request access to such personal information.

6.3 The right to have personal information corrected or deleted

A data subject may at any time request the correction, destruction or deletion of his/her personal information.

6.4 The right to object to the processing of personal information

A data subject has the right to object, on reasonable grounds relating to his/her particular situation, to the processing of his/her personal information.

6.5 The right to object to direct marketing

A data subject has the right to object to the processing of his/her personal information at any time for purposes of direct marketing and not to have his/her personal information processed for purposes of direct marketing by means of unsolicited electronic communications except as contemplated in section 69(1) of POPIA.[19]

6.6 The right not to be subject to automated processing of personal information

A data subject has the right not to be subject, under certain circumstances, to a decision which is based solely on the basis of the automated processing of his/her personal information intended to provide a profile of such person.

6.7 The right to complaints

A data subject may submit a complaint to the Information Regulator regarding the alleged interference with the protection of the personal information of any data subject or to submit a

[17] Chapter 3 of POPIA
[18] Section 5 of POPIA
[19] Application for the consent of a data subject for the processing of personal information for the purpose of direct marketing (Form 4) published in Government Notice No. R.1383 of 14 December 2018 (Government Gazette No. 42110 of 14 December 2018)

complaint to the Information Regulator in respect of a determination of an adjudicator as provided for in terms of section 74 of POPIA.

6.8 The right to civil proceedings

A data subject has the right to institute civil proceedings regarding the alleged interference with the protection of his/her personal information.

7. CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

The private body, responsible party, operators and any other person authorised to act on behalf of the private body shall at all times comply with the following conditions for the lawful processing of personal information:[20]

7.1 Accountability

The private body/responsible party shall take appropriate actions to ensure that the conditions outlined in Chapter 3 of POPIA and all the measures that give effect to such conditions, are complied with at the time of the determination of the purpose and means of the processing and during the processing itself. Appropriate actions to ensure compliance may include:

(a) Complying with best practices.
(b) Involving specialists/consultants for advice.
(c) Communicating requirements to data subjects.
(d) Scheduling regular internal audits.
(e) Using appropriate communication tools (telephone, electronic media, etc.).

7.2 Processing limitation[21]

Personal information shall be processed lawfully and in a reasonable manner that does not infringe the privacy of the data subject. Furthermore, it shall only be processed if, given the purpose for which it is processed, it is adequate, relevant and not excessive and 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 a 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 exercise of official authority vested in the private body or proper performance of a public law duty, 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.

The private body shall collect personal information directly from and with the consent of the data subject, except in cases where compliance would prejudice a lawful purpose of the collection, or

[20] Chapter 3 of POPIA
[21] Sections 9, 10,11 and 12 of POPIA

compliance is not reasonably practicable in the circumstances of the particular case, or as otherwise provided for in POPIA.[22]

7.3 Purpose specification

The responsible party shall only collect personal information for a specific, explicitly defined and lawful purpose related to the operating requirements, functions or activities of the private body and shall take appropriate steps to ensure that the data subject is aware of the purpose of the collection of the information unless otherwise provided.[23] Specific purposes for processing personal information may include:

(a) To gather contact information.
(b) To provide customers, business partners and other stakeholders with products and services or information in relation thereto.
(c) To conclude contractual arrangements.
(d) To monitor and/or record telephone calls and electronic transactions in order to accurately carry out instructions.
(e) For financial management such as processing of payments, invoices and claims.
(f) To confirm and verify a data subject's identity or to share specific personal information with a third party to perform verification or credit checks.
(g) In the interests of security and prevention of any fraudulent activity or malpractice.
(h) To conduct market or customer satisfaction research/surveys or for statistical analysis.
(i) For audit purposes and updating of records.
(j) In connection with legal proceedings.
(k) For recruitment and employment operations.
(l) For fulfilling our legitimate interests of improving and developing the quality of our products and services and enhancing customer experience.
(m) For business relationship management, for example networking and communication purposes, including to send newsletters, circulars or marketing promotions.
(n) To provide specific personal information to regulatory authorities, governmental departments, tax authorities and other persons/organizations in order for the private body to comply with laws and public duties.

The private body shall not retain records of personal information any longer than is necessary for achieving the purpose for which the information was collected or subsequently processed and any destruction or deletion of any records shall be undertaken as contemplated in POPIA[24] for example, the private body may retain certain personal information for longer when it is required or authorised by law, or when it reasonably requires the record for lawful purposes related to its activities and functions, or when required in terms of a contract.

In this regard the private body shall pay particular attention to specific requirements and timeframes in which certain personal information have to be retained as contemplated in Close Corporations Act, 1984 (No. 69 of 1984) read with the Institute of South African Chartered Accountants' Guide for the Retention of Records (May 2021).[25]

7.4 Further processing limitation

[22] Section12(2) of POPIA
[23] Section 18 of POPIA
[24] Section 14 of POPIA
[25] Search saica.co.za on the internet

Personal information shall only be further processed in accordance or compatible with the purpose for which it was initially collected or related purpose or purposes and as prescribed.[26]

The private body may disclose a data subject's personal information to any of its members, professional advisers, agents, suppliers or contractors insofar as reasonably necessary to perform the duties requested of them by the private body; however, third parties are not authorized to use or disclose any personal information except as necessary to perform services on the private body's behalf or to comply with legal requirements.

The private body may also disclose a data subject's personal information to a third party when necessary to protect any trademark, legal right, property or safety of its members, products or services.

The responsible party shall ensure that a third party with whom personal information is shared with agrees to keep such information confidential and appropriately secured.

The secondary processing of personal information shall not be implemented without the data subject's explicit consent.

7.5 Information quality

The responsible party shall take reasonably practicable steps with due regard to the type of the personal information and the purpose for which it is collected or further processed, to ensure that the personal information in its possession is complete, accurate, not misleading and updated.

Such steps shall include, but not limited to:

(a) Verifying and confirming the accuracy of the personal information with the data subject in person, in writing, by email or telephonically or a reliable independent source.
(b) Obtaining personal information from third parties for verification and vetting purposes such as referees, professional institutions/associations, affiliated companies, etc.
(c) Properly documenting the purpose for processing and the justification for the lawful basis thereof.
(d) Properly articulating the legal justification for processing varying types of personal information (accounts information, employment records, etc.).
(e) Proper record keeping of processing activities, who has access to the information, description of the relationships between the responsible party and data subject and the types of personal information.

7.6 Openness

The responsible party shall maintain the documentation of all processing operations under its responsibility in accordance with PAIA.[27]

The responsible party shall take reasonably practicable steps when personal information is collected that the data subject is aware of, including but not limited to:[28]

[26] Section 15 of POPIA
[27] As referred to in Section 14 or 51 of PAIA, as the case may be
[28] Section 18 of POPIA

(a) The fact that the information is being collected.
(b) Providing reasons for the purpose for which the information is being collected.
(c) The intended recipients of the information.
(d) Identifying the responsible party (name and address, etc.) that is collecting the information.
(e) Whether the collection of the information is authorised or required by a specific law or is provided voluntary or mandatory.
(f) The consequences, if any, for that data subject if all or any part of the requested information is not provided.
(g) The rights of access to, and correction of, the information provided.

7.7 Security safeguards

The responsible party shall 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:

(a) Loss of damage to or unauthorised destruction of personal information.
(b) Unlawful access to or processing of personal information.

The responsible party or an operator or anyone processing personal information on behalf of the private body shall be required to process such information only with the knowledge or authorisation of the private body and to treat personal information as confidential unless required by law or in the course of the proper performance of their duties.

A responsible party shall conclude a written contract with any operator which processes personal information on behalf of the responsible party stipulating, among others, that:

(a) The operator must establish and maintain any security measures introduced by the responsible party to secure the integrity and confidentiality of personal information.
(b) The operator must notify the responsible party immediately where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person.

When managing personal information integrity and confidentiality, the private body shall have regard to specific physical, electronic and managerial precautionary measures which may include:

Encrypting sensitive files
To render sensitive personal information unreadable to anyone except those who have the appropriate password or key.

Managing access and usage
Ensuring that access is only authorized and granted to those who have a "need to know" and that users authenticate access with strong passwords and, where practical, two-factor authentication. Access lists and passwords shall be periodically reviewed and promptly revoked or when necessary.

Physically securing devices and paper documents
Controlling access to personal information shall include both digital and physical access. Devices and paper documents shall be protected from misuse or theft by not leaving it unattended in public locations and storing it in locked areas.

Secure disposing of personal information, devices and paper records
The following measures shall be implemented with due regard to the type of personal information:

(a) When personal information is no longer necessary for the purpose it was initially processed, it shall be deleted or disposed of appropriately.
(b) Sensitive personal information such as account numbers, physical or mental health status, financial and criminal history, shall be securely erased to ensure that it cannot be recovered and misused.
(c) Devices that were used to store sensitive information shall be destroyed or securely erased to ensure that its previous contents cannot be recovered and misused.
(d) Paper documents containing personal information shall be shredded rather than dumped into trash or recycling bins.

Managing data acquisition
When collecting personal information, the responsible party shall be conscious of how much information is actually needed and must carefully consider privacy and confidentiality in the acquisition process. Acquiring sensitive personal information shall be processed only if absolutely necessary and care shall be taken to minimise confidentiality risk by reducing the amount of personal information being collected.

Managing data utilization
Confidentiality risks shall be reduced by using sensitive personal information only as approved by the responsible party and as necessary. Misusing sensitive data violates the privacy and confidentiality of such information and of the data subject it represents.

Managing computers and networks
Computer management shall include various essential security practices such as basic cybersecurity hygiene by using anti-virus software, passcodes and enabling firewalls.

The private body shall on an on-going basis continue to review its security controls and related processes to ensure that personal information remains secure.

7.8 Data subject participation

A data subject having provided adequate proof of identity may request a responsible party to confirm, free of charge:

(a) Whether or not the responsible party holds personal information about the data subject.
(b) To make available the record or a description of the personal information about the data subject held by the responsible party, including information about the identity of all third parties or categories of third parties, who have or have had access to the information.

A responsible party may or must refuse, as the case may be, to disclose any information requested to which the grounds for refusal of access to records set out in PAIA apply.

A data subject may in the prescribed manner request a responsible party to:
(a) Correct or delete personal information about the data subject that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.
(b) Destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain.

8. PROCESSING OF PERSONAL INFORMATION SUBJECT TO PRIOR AUTHORIZATION

The responsible party shall notify the Information Regulator if he/she is processing or intends to process any personal information in relation to, amongst others:[29]

(a) Unique identifiers of data subjects for a purpose other than the one for which the identifier was specifically intended at collection and with the aim of linking the information together with information processed by other responsible parties (examples of unique identifiers are bank account numbers or any account number, ID number, employee number, telephone or cell phone number).
(b) Criminal behaviour or an unlawful or objectionable conduct of data subjects on behalf of third parties for purposes such as criminal record enquiry, reference checking pertaining to the past conduct or disciplinary action taken against a data subject.
(c) Credit reporting.
(d) Transfer of the special personal information or personal information of children to a third party in a foreign country that does not provide an adequate level of protection for the processing of personal information.

9. DESCRIPTION OF THE CATEGORIES OF DATA SUBJECTS, PERSONAL INFORMATION IN RELATION THERETO AND RECIPIENTS OF INFORMATION

The private body in the normal course of its business operations may process personal information of the following categories of data subjects, but not necessarily limited thereto depending on the circumstances of the case:[30]

Categories of data subjects	Categories of personal information relating to the data subjects	Recipients to whom the personal information may be supplied
Employees	Bank account details Disability Disciplinary record Education Emails/Correspondence Employment & criminal history Full names & ID number Language, gender & race Marital status Physical or mental health Physical, postal & email address Telephone numbers References Remuneration & leave records	Company directors/reception Department of Labour Financial Institutions Office staff SA Revenue Services
CC members/directors	Bank account details Emails/Correspondence Full names Gender	Accountants CC members/Directors Customers/business partners Financial Institutions Medical/Pension Fund

[29] Sections 57, 58 and 59 of POPIA read with the Guidance Note on Application for Prior Authorisation published on the Information Regulator's website https://justice.gov.za/inforeg/
[30] Section 51(1)(c)(ii) and (iii) of PAIA

	ID Number Marital Status Physical & postal & email address Telephone numbers	Office staff SA Revenue Services Companies and Intellectual Property Commission (CIPC) Suppliers/service providers
Suppliers/service providers	Bank account details Emails/Correspondence Business/Company name Physical, postal & email address Price schedules Products and services Telephone numbers Transactional records (invoices, payments, etc.) VAT details	Accountants Auditors CC members/directors Reservation/Office staff
Customers/business partners	Bank account & VAT numbers Business/Company name Emails/Correspondence Full names & ID number Work title Physical, postal & email address Telephone numbers Transactional records (accounts & payments, etc.)	Accountant Attorneys Auditors CC members/directors Debt collection agencies Office staff SA Revenue Services
Visitors/Guests	Bank account /Credit Card details Emails/correspondence Full names ID/Passport number Physical, postal & email address Reservation details Telephone numbers Transactional records (invoices, payments, etc.)	Accountants Attorneys/Debt collection agencies Auditors CC members/directors Reservation/Office staff

10. TRANSFERS OF PERSONAL INFORMATION OUTSIDE SOUTH AFRICA

The responsible party shall not transfer personal information about a data subject to a third party who is in a foreign country unless:[31]

(a) The person receiving the information is subject to similar laws.
(b) The data subject has agreed to the transfer of the information.
(c) Such transfer is part of the performance of a contract which the data subject is a party.
(d) Transfer is for the benefit of the data subject and it is not reasonably practicable to obtain his/her consent which consent would likely be given.

However, should it be necessary in accordance with the private body's operating requirements to transfer personal information about a data subject to a third party in a foreign country which do

[31] Section 72 of POPIA.

not have approval as contemplated in POPIA, the private body shall first establish legal grounds justifying such transfer and/or in consultation with the Information Regulator.

11. INFORMATION OFFICER[32]

The Head of the private body[33] is designated as Information Officer and as such the responsible party as contemplated in POPIA.

The duties and responsibilities of the Information Officer include:[34]

(a) The encouragement of compliance by the private body with the conditions for the lawful processing of personal information.
(b) Dealing with requests, objections and complaints made to the private body pursuant to POPIA.
(c) Working with the Information Regulator in relation to investigations conducted pursuant to Chapter 6 of POPIA in relation to the private body.
(d) In general, ensuring compliance by the private body with the provisions of POPIA.
(e) Other duties as may be prescribed.

The Information Officer must, in addition to the duties and responsibilities referred to in POPIA and PAIA, ensure that:[35]

(a) A compliance framework is developed, implemented, monitored and maintained.[36]
(b) A personal information impact assessment is done to ensure that adequate measures and standards exist in order to comply with the conditions for the lawful processing of personal information.
(c) A manual is developed, monitored, maintained and made available as prescribed in section 14 (for public bodies) or section 51 (for private bodies) of PAIA.
(d) Internal measures are developed together with adequate systems to process requests for personal information or access thereto.
(e) Internal awareness sessions are conducted regarding the provisions of POPIA, the regulations made in terms thereof, codes of conduct or information obtained from the Information Regulator.

The Information Officer has been registered with the Information Regulator as prescribed.[37]

---

[32] Read in conjunction with the Guidance Note on Information Officers and Deputy Information Officers published on the Information Regulator's website https://justice.gov.za/inforeg/
[33] See Part Two, paragraph 3, of this/her Manual
[34] Section 55(1) of POPIA
[35] Regulations relating to the Protection of Personal Information (Government Notice No.R.1383 of 14 December 2018)
[36] If necessary insofar as it is not covered in this Policy Manual
[37] Section 55(2) of POPIA