



COMPLIANCE MANUAL FOR THE IMPLEMENTATION OF THE
PAIA (PROMOTION OF ACCESS TO INFORMATION ACT) and
POPIA (PROTECTION OF PERSONAL INFORMATION ACT)

CONTENTS:

A. Introduction	Page 2
B. Our Undertaking to our Clients	Page 2
C. Our Client's Rights	Page 4
D. Information Officer	Page 4
E. Human Rights Commission Guide	Page 6
F. Information Available in Terms of the Act	Page 7
G. Processing of Personal Information	Page 10
Categories of Data Subjects	Page 10
Categories of Recipients	Page 11
Security Safeguards	Page 11
Security Breaches	Page 12
Clients Requesting Records	Page 13
Objection, Withdrawal or Correction of PI	Page 14
Special Personal Information	Page 14
Processing of Personal Information of Children	Page 14
Circumstances Requiring Prior Authorization	Page 14
Means of Collection and Use of Personal Information	Page 15
Transborder Information Flows	Page 16
Offences and Penalties	Page 16
H. Schedule of Annexures and Forms	Page 17

A. INTRODUCTION

The Protection of Personal Information Act (POPI) is intended to balance two competing interests. These are:

1. Our individual constitutional rights to privacy (which requires our personal information to be protected); and
2. The needs of our society to have access to and to process (work with) our personal information for legitimate purposes, including the purpose of doing business.

This Compliance Manual sets out the framework for our company's compliance with POPI.

Where reference is made to the "processing" of personal information, this will include any activity in which the information is worked with, from the time that the information is collected, up to the time that the information is destroyed, regardless of whether the information is worked with manually, or by automated systems.

3. It should be noted that POPIA defines consent as:
 - 3.1 Any voluntary, specific and informed expression of will.
 - 3.2 Processing as collection, receipt, recording, organization, storage, merging and linking.
 - 3.3 Personal information as any information relating to not only a natural person but also a company or legal entity, but not limited to:
 - 3.3.1. Names, addresses, telephone numbers, email addresses.
 - 3.3.2. Information about age, race, gender, appearance, characteristics, sexual orientation, political convictions, religious beliefs, language.
 - 3.3.3. Health data such as physical or mental health, well-being, disabilities.
 - 3.4 Online identifiers such email addresses, IP addresses, cookies, unique IDs, search and browser history.
 - 3.5 Location data.

B. OUR UNDERTAKINGS TO OUR CLIENTS:

1. We undertake to follow POPI at all relevant times and to process personal information lawfully and reasonably, so as not to infringe unnecessarily on the privacy of our clients.
2. We undertake to process information only for the purpose for which it is intended, to enable us to do our work, as agreed with our clients.
3. Whenever necessary, we shall obtain consent to process personal information.

4. Where we do not seek consent, the processing of our client's personal information will be following a legal obligation placed upon us, or to protect a legitimate interest that requires protection.
5. We shall stop processing personal information if the required consent is withdrawn, or if a legitimate objection is raised.
6. We shall collect personal information directly from the client whose information we require, unless:
 - 6.1 the information is of public record, or
 - 6.2 the client has consented to the collection of their personal information from another source, or
 - 6.3 where requesting consent is not reasonably practical in the circumstances.
7. We shall advise our clients of the purpose of the collection of the personal information.
8. We shall retain records of the personal information we have collected indefinitely unless the client has objected or withdrawn their consent or instructed us otherwise. If the client objects to indefinite retention of its Personal Information we shall retain the Personal Information records to the extent permitted or required by law.
9. We shall destroy or delete records of the personal information (so as to de-identify the client) as soon as reasonably possible after the time period for which we were entitled to hold the records have expired.
10. We shall restrict the processing of personal information:
 - 10.1 where the accuracy of the information is contested, for a period sufficient to enable us to verify the accuracy of the information;
 - 10.2 where the purpose for which the personal information was collected has been achieved and where the personal information is being retained only for the purposes of proof;
 - 10.3 where the client requests that the personal information is not destroyed or deleted, but rather retained; or
 - 10.4 where the client requests that the personal information be transmitted to another automated data processing system.
11. The further processing of personal information shall only be undertaken:
 - 11.1 if the requirements of paragraphs 3; 6.1; 6.2; 6.3 above have been met;
 - 11.2 where the further processing is necessary because of a threat to public health or public safety or to the life or health of the client, or a third person;
 - 11.3 where the information is used for historical, statistical or research purposes and the identity of the client will not be disclosed; or
 - 11.4 where this is required by the Information Regulator appointed in terms of POPI.
12. We undertake to ensure that the personal information which we collect and process is complete, accurate, not misleading and up to date.

13. We undertake to retain the physical file and the electronic data related to the processing of the personal information.
14. We undertake to take special care with our client's bank account details (if applicable), and we are not entitled to obtain or disclose or procure the disclosure of such banking details unless we have the client's specific consent.
15. **Annexure 1 a, b, c, d & e** referred to in Section H are our Golf; Social, Gym & Ambrose Lofts Membership Forms, which every new member is required to complete prior to the acceptance of membership. It also advises them of our commitment to them in terms of POPI.

C. OUR CLIENT'S RIGHTS

1. In cases where the client's consent is required to process their personal information, this consent may be withdrawn.
2. In cases where we process personal information without consent to protect a legitimate interest, to comply with the law or to pursue or protect our legitimate interests, the client has the right to object to such processing.
3. All clients are entitled to lodge a complaint regarding our application of POPI with the Information Regulator.
4. Form 1 a, b, c, d, e referred to in Section B. 15 and Section H below, shall be completed by each client on request for membership, to obtain the client's consent to process their personal information.

D. INFORMATION OFFICER

The Owner / General Manager is by virtue of appointment accountable for legal compliance and governance. To assist the General Manager with the administration of defined controls to ensure compliance with PAIA and POPIA, the Administration Manager is the Designated Information Officer of Zwartkop Country Club. The Administration Assistant; the Administration Assistant of Zwartkop Catering and the Campus Head of The Golf Management Campus have been designated as Deputy Information Officers.

Requests pursuant to the provisions of the Act should be directed as follows:

Name of Organisation	Zwartkop Country Club
Registration Number	2001/012010/07
Registered Address	Old Johannesburg Rd, Clubview, Centurion
Postal Address	P.O. Box 14636, Lyttelton, 0140
Telephone Number	+27 12 6654-1144
Designated Information Officer	Kotie Venter
Email address	kotie@zwartkopcc.co.za

Deputy Information Officer	Queen Bukhali
Email address	admin@zwardkopcc.co.za
Deputy Information Officer	Joanita Verster (Golf Management Campus)
Email address	mentor@golfmanagementcampus.co.za
Website	www.zwardkopcountryclub.co.za
Deputy Information Officer	Ina Rouse (Zwardkop Catering)
Email address	admin@zwardkopcatering.co.za
Website	www.zwardkopcountryclub.co.za

1. The Information Officer has been nominated and authorised by the Owner, in writing. Such authorisation has been made on the form in **Annexure 2** in Section H. Our Information Officer's responsibilities include:
 - 1.1 Ensuring compliance with POPI.
 - 1.2 Dealing with requests which we receive in terms of POPI.
 - 1.3 Working with the Information Regulator in relation to investigations.
2. Our Information Officer will designate in writing as many Deputy Information Officers as are necessary to perform the tasks mentioned in paragraph 1 above. Such designation shall be done by the completion of the prescribed form a copy of which is an annexure to this Compliance Manual, see **Annexure 3**, Section H.
3. Our Information Officer and our Deputy Information Officers must register themselves with the Information Regulator prior to taking up their duties, see **Annexure 4**, Section H.
4. In carrying out their duties, our Information Officer must ensure that:
 - 4.1 this Compliance Manual is implemented;
 - 4.2 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;
 - 4.3 that this Compliance Manual is developed, monitored, maintained and made available;
 - 4.4 that internal measures are developed together with adequate systems to process requests for information or access to information;
 - 4.5 that internal awareness sessions are conducted regarding the provisions of POPI, the Regulations, codes of conduct or information obtained from the Information Regulator; and
 - 4.6 that copies of this manual are provided to persons at their request, hard copies to be provided upon payment of a fee (to be determined by the Information Regulator).

5. Guidance notes on Information Officers have been published by the Information Regulator (on 1 April 2021) and our Information Officer and deputy Information Officers must familiarize themselves with the content of these notes. See **Annexure 4**, Section H.

E HUMAN RIGHTS COMMISSION (HRC) GUIDE

The Human Rights Commission has been tasked with the administration of the PAIA Act. Section 10 of the PAIA Act requires the South African Human Rights Commission (SAHRC) to publish a guide which is intended to assist users in the interpretation of the PAIA Act and how to access the records of private and public bodies and the remedies available in law regarding a breach of any of the provisions of the PAIA Act.

The guide will contain the following information:

1. The objects of the Act;
2. Particulars of the information officer of every public body;
3. Particulars of every private body as are practicable;
4. The manner and form of a request for access to information held by a body;
5. Assistance available from both the information officers and the SAHRC in terms of this Act;
6. All remedies in law regarding acts, omissions, rights and duties, including how to lodge an internal appeal and a court application;
7. Schedules of fees to be paid in relation to requests for access to information;
8. Regulations made in terms of the Act.

Copies of this guide are available from SAHRC. Enquiries regarding the Guide and relating to body can be addressed to the SAHRC, the contact details of which are as follows:

Post	The South African Human Rights Commission: PAIA (Promotion of Access to Information Act) Unit Research and Documentation Department Private Bag 2700 Houghton 2041
Telephone Number :	+27 (11) 484 8300/ +27 11 877 3600
Fax :	+27 (11) 484 7146/ +27 11 403 0625
Email :	PAIA@sahrc.org.za/ section51.paia@sahrc.org.za
Website :	http://www.sahrc.org.za

F INFORMATION AVAILABLE IN TERMS OF THE ACT

Zwartkop Country Club will protect the confidentiality of information provided to it by third parties, subject to its obligations to disclose information in terms of any applicable law or regulation or a court order requiring disclosure of information. If access is requested to a record that contains information about a third party, Zwartkop Country Club is obliged to attempt to contact such third party to inform him/her/it of the request.

Zwartkop Country Club will give the third party an opportunity of responding by either consenting to the access or by providing reasons why the access should be denied. In the event that the third-party furnishing reasons for the support or denial of access, the Deputy Information Officer will consider these reasons in determining whether access should be granted to the requestor or not.

1 Records automatically available - [section 51(1) (c)]

At this stage no notice(s) has/have been published in terms of section 52 of the PAIA on the categories of records that are automatically available without a person having to request access in terms of the PAIA.

Records that are automatically available at the registered office of on payment of the prescribed fee for reproduction are:

- Records of Zwartkop Country Club lodged in terms of government requirements such as the Registrar of Deeds;
- Documentation and information relating to Zwartkop Country Club which is held by the Companies and Intellectual Properties Commission in accordance with the requirements set out in set out in section 25 of the Companies Act 71 of 2008;
- Services Brochures and Promotions; and
- News and other Marketing Information, media releases, public relations policies and procedures, service and product information
- Certain other information is also made available on said website from time to time.

2. Information Available on Request Section (51(1)(e))

Information that is not readily available may be requested in accordance with the procedure prescribed in terms of the Act. Please note that a requestor is not automatically allowed access to these records and access to same may, or can be refused in accordance with the provisions of the Act.

Subjects and Categories of Records that may be held with the Company are listed in **Annexure 5**, Section H.

3. Records that are not automatically available

Records of the Company which are not automatically available must be requested in terms of the procedure set out in this PAIA Manual or the Regulations as set out in terms of POPIA and which may be subject to the restrictions and right of refusal to access as provided for in the PAIA and in POPIA.

No request shall be accepted telephonically nor shall any information be supplied telephonically. Only the Information officer or any Deputy Information officer appointed shall have the mandate to disclose information in terms of this manual.

4. Information Available In Terms Of Other Legislation [Section 51(1) (D)]

A list of possible records kept with regards to Information of Other Legislation applicable to our operations, are listed in **Annexure 5**, Section H.

While we endeavor to supply you with a complete list of applicable legislation it is possible that the list may be incomplete. The list will be updated accordingly when brought to our attention that existing or new legislation allows a requester access on a basis other than that set out in the PAIA or POPIA Acts.

5. Procedure for requesting access to the above information

See the Promotion of Access to Information Act No. 2 of 2000 (Section 53) and Government Notice No. R. 187 of 15 February 2002, Annexure B.

Records held by Zwartkop Country Club may be accessed, on request, only once the requirements for access have been met. A requester is any person making a request for access to a record of the Company and in this regard, the Act distinguishes between two types of requesters.

The requester must use the prescribed form to make the request for access to a record. This must be made to the head of the private body. This request must be made to the address or electronic mail address of the body concerned Section 53 (1).

The requester must provide sufficient detail on the request form to enable the head of the private body to identify the record and the requester. The requester should also indicate which form of access is required. The requester should also indicate if any other manner is to be used to inform the requester and state the necessary particulars to be so informed. Section 53(2)(a) and (b) and (c).

The requester must identify the right that is sought to be exercised or to be protected and provide an explanation of why the requested record is required for the exercise or protection of that right. Section 53(2)(d).

If a request is made on behalf of another person, the requester must then submit proof of the capacity in which the requester is making the request to the satisfaction of the head of the private body. Section 53(2)(f).

6. Fees

The Act provides for two types of fees, namely:

- A request fee, which will be a standard fee; and
- An access fee, which must be calculated by considering reproduction costs, search and preparation time and costs, as well as postal costs.

When the request is received by the Deputy Information Officer of the Company, such person shall by notice require the requester to pay the prescribed request fee, if any, before further processing of the request.

If a requester requires access to records of his/her Personal Information, there shall be no request fee payable. However, the requester must pay the prescribed access and reproduction fees for such Personal Information. Every other requester, who is not a personal requester, must pay the required request fee.

A requester who seeks access to a record containing personal information about that requester is not required to pay the request fee. Every other requester, who is not a personal requester, must pay the required request fee.

The head of the private body must notify the requester (other than a personal requester) by notice, requiring the requester to pay the prescribed fee (if any) before further processing the request. Section 54(1).

The fee that the requester must pay to a private body is R50,00. The requester may lodge an application to the court against the tender or payment of the request fee. Section 54(3)(b).

After the head of the private body has made a decision on the request, the requester must be notified in the required form.

If the request is granted then a further access fee must be paid for the search, reproduction, preparation and for any time that has exceeded the prescribed hours to search and prepare the record for disclosure. Section 54(6).

Details of these fees are contained in **Annexure 8** in Section H.

7. Particulars in terms of section 51 of the act

On 9 March 2001 the PAIA Act came into effect. The Act seeks to advance a culture of transparency and accountability in both public and private bodies. The legislation was enacted as a direct response to Section 32(2) of the Constitution of South Africa – the right of access to information – which requires that the Government implements laws in an effort to make information pertaining to public and private bodies more accessible to all.

The Act gives effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights. Where a request is made in terms of the PAIA, the body to whom the request is made is obliged to release the information, except where the PAIA expressly provides that the information may or must not be released.

One of the main requirements specified in the PAIA is the compilation of a manual that provides information on both the types and categories of records held by the public or private body. In terms of the PAIA, the Company is regarded as a “private body” and therefore the requirements regarding access must be in compliance with the provisions of the PAIA relevant to private bodies and more in particular Section 51 of the PAIA.

In compliance with Section 51 of the PAIA, this Manual sets out the following details:

- a) The Company’s contact details including, physical and postal addresses, telephone number, electronic mail address of the person tasked in terms of this Code of Conduct;

- b) Information on how to obtain and access this Code of Conduct and a guide on how to use it;
- c) Categories of information held by the Company that is available without a person having to formally request such details in terms of the PAIA;
- d) Categories of information held by the Company that is available in accordance with other legislation and which, subject to the PAIA, may be made available by the Company on receipt of and consideration of a formal request, made in terms of the PAIA; and
- e) Sufficient information to facilitate a request for access to records and a description of the subjects on which records are available from the Company.

Adherence to these requirements entails not only compilation of the external manual but also compliance with the general provisions stated in the PAIA Act.

G. PROCESSING OF PERSONAL INFORMATION

1. Purpose of Processing

Zwartkop Country Club uses the Personal Information under its care in the following ways:

- Conducting credit reference checks and assessments
- Administration of agreements
- Providing products and services to customers
- Discounting and asset funding purposes
- Detecting and prevention of fraud, crime, money laundering and other malpractice
- Conducting market or customer satisfaction research
- Marketing and sales
- In connection with legal proceedings
- Staff administration
- Keeping of accounts and records
- Complying with legal and regulatory requirements
- Profiling data subjects for the purposes of direct marketing

2. Categories of Data Subjects and their Personal Information

Zwartkop Country Club may possess records relating to suppliers, shareholders, contractors service providers, staff and customers:

Entity Type	Personal Information Processed
Customers - Natural Persons	Names; contact details; physical and postal addresses; date of birth; ID number; tax related information; nationality; gender; race (optional); confidential correspondence
Customers – Juristic Persons / Entities	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information

Contracted Service Providers	Names of contact persons; name of legal entity; physical and postal address and contact details; financial information; registration number; founding documents; tax related information; authorised signatories; beneficiaries; ultimate beneficial owners; shareholding information; BBBEE information
Employees / Directors	Gender; pregnancy; marital status; colour, race; age; language; education information; financial information; employment history; ID number; physical and postal address; contact details; opinions; criminal record; well-being

3. Categories of Recipients for Processing the Personal Information

Zwartkop Country Club may share the Personal Information with its agents, affiliates, and associated companies who may use this information to send the Data Subject information on products and services. It may also supply the Personal Information to any party to whom it may have assigned or transferred any of its rights or obligations under any agreement, and/or to service providers who render the following services:

- Capturing and organising of data;
- Storing of data;
- Sending of emails and other correspondence to customers;
- Conducting due diligence checks;
- Administration of the Medical Aid and Pension Schemes.

4. Security Safeguards

4.1. In order to secure the integrity and confidentiality of the personal information in our possession, and to protect it against loss or damage or unauthorised access, we continue to implement the following security safeguards:

4.1.1 Our premises where records are kept are protected by access control.

4.1.2 Archived files are stored behind locked doors and have access control to the storage facilities. Offices and cupboards are locked.

4.1.3 All the user terminals on our internal computer network, and our server, are protected by passwords which are changed on a regular basis.

4.1.4. Our email / website infrastructure complies with industry standard security safeguards, and meets the General Data Protection Regulation (GDPR), which is standard in the European Union.

4.1.5 Vulnerability assessments are carried out regularly on our digital infrastructure to identify weaknesses in our systems and to ensure we have adequate security in place.

4.1.6 We have a MikroTik Firewall in place to protect the data on our individual computer units and the server and antivirus protection on our systems.

4.1.7 Our server backs up both to a hard drive and via the cloud. All hard copy information will be reconstructed as and when necessary.

4.1.8 Systems and programs are updated monthly by our IT service provider.

4.1.9 Our staff must be trained to carry out their duties in compliance with POPI, and this training must be ongoing.

4.1.10 It is a term of the contract with every staff member that they must maintain full confidentiality in respect of all of our clients' affairs, including our clients' personal information

4.1.11 Employment contracts for staff whose duty it is to process a client's personal information, includes an obligation on the staff member (1) to maintain the Company's security measures, and (2) to notify their manager/supervisor immediately if there are reasonable grounds to believe that the personal information of a client has been accessed or acquired by any unauthorised person. See **Annexure 6**, Section H for the relevant addendum/clause and /or Declaration Form on Access to Personal Information.

4.1.12 The processing of the personal information of our staff members must take place in accordance with the rules contained in the relevant labour legislation.

4.1.13 The digital work profiles and privileges of staff who have left out employ must be properly terminated.

4.1.14 The personal information of clients and staff must be destroyed timeously in a manner that de-identifies the person.

4.1.15 Outsourced Service Providers who process Personal Information on our behalf are contracted to implement security controls.

4.2. These security safeguards must be verified on a regular basis to ensure effective implementation, and these safeguards must be continually updated in response to new risks or deficiencies.

5. Security Breaches

5.1. Should it appear that the personal information of a client has been accessed or acquired by an unauthorised person, we must notify the Information Regulator and the relevant client/s as soon as reasonably possible.

5.2. Such notification must be given to the Information Regulator first as it is possible that they, or another public body, might require the notification to the client/s be delayed.

5.3. The notification to the client must be communicated in writing in one of the following ways, with a view to ensuring that the notification reaches the client:

5.3.1 by mail to the client's last known physical or postal address;

5.3.2 by email to the client's last known email address;

5.3.3 by publication on our website or in the news media; or

5.3.4 as directed by the Information Regulator.

- 5.4 This notification to the client must give sufficient information to enable the client to protect themselves against the potential consequences of the security breach, and must include:
- 5.4.1 a description of the possible consequences of the breach;
 - 5.4.2 details of the measures that we intend to take or have taken to address the breach;
 - 5.4.3 the recommendation of what the client could do to mitigate the adverse effects of the breach; and
 - 5.4.4 if known, the identity of the person who may have accessed, or acquired the personal information.

6. Clients Requesting Records

- 6.1. On production of proof of identity, any person is entitled to formally request that we confirm whether or not we hold any personal information about that person in our records.
- 6.2. If we hold such personal information, on request, we shall provide the person with the record, or a description of the personal information, including information about the identity of all third parties or categories of third parties who have or have had access to the information. We shall do this within a reasonable period of time, in a reasonable manner and in an understandable form.
- 6.3. A client requesting such personal information must be advised of their right to request to have any errors in the personal information corrected, which request shall be made on the prescribed application form.
- 6.4. In all cases where the disclosure of a record will entail the disclosure of information that is additional to the personal information of the person requesting the record, the written consent of the Information Officer (or his delegate) will be required, and that person shall make their decision having regard to the provisions of Chapter 4 of Part 3 of the Promotion of Access to Information Act.
- 6.5. If a request for personal information is made and part of the requested information may, or must be refused, every other part must still be disclosed. The completion and submission of a request does not automatically allow the requester access to the requested record. An application for access to a record is subject to certain limitations if the requested record falls within a certain category as specified within part 3 Chapter 4 of the Act.
- 6.6. If you wish to request access to any of the above categories of information you are required to complete a request form as set out in **Annexure 7** in Section H.
- 6.7. There is a prescribed fee (payable in advance) for requesting and accessing information in terms of the Act. Details of these fees are contained in **Annexure 8** in Section H.

7. The Objection; Withdrawal Or Correction Of Personal Information
 - 7.1. A client is entitled to object to, or require us to withdraw, correct or delete personal information that we have, which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or which has been obtained unlawfully.
 - 7.2. A client is also entitled to require us to destroy or delete records of personal information about the client that we are no longer authorised to retain.
 - 7.3. Any such Objection must be made on the prescribed form, **Annexure 9** in Section H. A request for withdrawal of information must be made on the prescribed form, **Annexure 10** in Section H, while any request for us to Correct, Destroy or Delete records of personal information must be made on the prescribed form, **Annexure 11** in Section H.
 - 7.4. Upon receipt of such a lawful request, we must comply as soon as reasonably practicable.

8. Special Personal Information
 - 8.1. Special rules apply to the collection and use of information relating to a person's religious or philosophical beliefs, their race or ethnic origin, their trade union membership, their political persuasion, their health or sex life, their biometric information, or their criminal behaviour.
 - 8.2. We shall not process any of this Special Personal Information without the client's consent, or where this is necessary for the establishment, exercise or defense of a right or an obligation in law.

9. The Processing Of Personal Information Of Children
 - 9.1. We may only process the personal information of a child if we have the consent of the child's parent or legal guardian.

10. Circumstances Requiring Prior Authorisation
 - 10.1. In the following circumstances, we will require prior authorisation from the Information Regulator before processing any personal information:
 - 10.1.1 In the event that we intend to utilise any unique identifiers of clients (account numbers, file numbers or other numbers or codes allocated to clients for the purposes of identifying them in our business) for any purpose other than the original intention, or to link the information with information held by others;
 - 10.1.2 if we are processing information on criminal behaviour or unlawful or objectionable conduct;
 - 10.1.3 if we are processing information for the purposes of credit reporting;
 - 10.1.4 if we are transferring special personal information or the personal information of children to a third party in a foreign country, that does not provide adequate protection of that personal information.

10.2. The Information Regulator must be notified of our intention to process any personal information as set out in paragraph 10.1 above prior to any processing taking place and we may not commence with such processing until the Information Regulator has decided in our favour. The Information Regulator has 4 weeks to make a decision but may decide that a more detailed investigation is required. In this event the decision must be made in a period as indicated by the Information Regulator, which must not exceed 13 weeks. If the Information Regulator does not make a decision within the stipulated time periods, we can assume that the decision is in our favour and commence processing the information.

11. Means Of Collection And Use Of Personal Information

11.1. We may only approach clients using their personal information, if we have obtained their personal information in the context of providing services associated with our business to them, and we may then only market services related to the golf club to them.

11.2. If not indicated on the original Membership Application Form, (**Annexure 1** in Section H), then a request for Consent to Process Personal Information and / or to Consent to Receive the electronic newsletters / email communication and / or direct marketing must be made on the prescribed forms – under **Annexure 12 & Annexure 13** under Section H.

11.3. All electronic newsletters / email communication and / or direct marketing must disclose our identity and contain an address or other contact details to which the client may send a request that the communications cease.

11.4. The following direct means of collection of Personal Information have been identified at Zwartkop CC and their use / security / retention or deletion is noted as follows:

11.4.1 Website Browsing and access to Clubhouse WIFI:

When visiting the Website or WIFI services, our servers automatically record “non-personal” information that your browser sends. This data may include information such as your device’s IP address, browser type and version, operating system type and version, language preferences or the webpage you were visiting before you came to our Website, pages of our Website that you visit, the time spent on those pages, information you search for on our Website, access times and dates, and other statistics.

11.4.2 Email Communication and Electronic Newsletters:

Membership Application Forms ask for consent for email / newsletter and SMS communication. All electronic newsletter communication requires manual subscription by the client and provides an unsubscribe option. In addition, any person can request removal from receiving communication.

11.4.3 Mobile App:

The My Home Club App requires manual subscription by the client themselves and allows them to unsubscribe from the service.

11.4.4 Membership Application Forms (Golf, Gym, Social) – Hard Copy / Online:

Membership Forms act as the contract of consent between the client and Zwartkop Country Club. No information is shared without prior consent by the

Client. All hardcopy contracts are securely stored and only for the period of time required.

11.4.5 Clubmaster Database:

The membership database is digitally stored on the Clubmaster system and is only accessible to the Information Officer and the Deputy Information Officer.

11.4.6 Handicaps Network Africa / SAGA / GNGU:

All information stored on HNA's system is with the prior consent of the Client in servicing their handicap. Information is digitally stored on the HNA system and is only accessible to those dealing directly with handicaps.

11.4.7 ZGEHOA Gate Access / Biometrics:

All information – biometric or other, stored on the Zwartkop Home Owners Association system, is with the prior consent of the Client and is protected under the ZHOA POPI Policy.

11.4.8 Staff Database & Records:

All Staff information – biometric or other, is stored either in a secure strong room or on the Zwartkop server. All information is provided with the prior consent of the Employee.

12. Transborder Information Flows

12.1. We may not transfer a client's personal information to a third party in a foreign country, unless:

12.1.1 the client consents to this, or requests it; or

12.1.2 such third party is subject to a law, binding corporate rules or a binding agreement which protects the personal information in a manner similar to POPI, and such third party is governed by similar rules which prohibit the onward transfer of the personal information to a third party in another country

13. Offences And Penalties

13.1. POPI provides for serious penalties for the contravention of its terms. For minor offences a guilty party can receive a fine or be imprisoned for up to 12 months. For serious offences the period of imprisonment rises to a maximum of 10 years. Administrative fines for the company can reach a maximum of R10 million.

13.2. Breaches of this Compliance Manual will also be viewed as a serious disciplinary offence.

13.3. It is therefore imperative that we comply strictly with the terms of this Compliance Manual and protect our client's personal information in the same way as if it was our own.

13.4 You may lodge a complaint with the Regulator. You may also lodge a complaint with the RESPONSIBLE PARTY by contacting the Information Officer referred to on Page 4.

H. ANNEXURES

1. Membership Form
 - a) Golf Membership Form
 - b) Gym Membership
 - c) Social Membership
 - d) Ambrose Lofts Golf & Gym Membership
 - e) Ambrose Lofts Social Membership
2. Authorisation of Information Officer.
3. Designation and Delegation to Deputy Information Officer Client's
4. Information Officer's registration Form & Guidance Notes.
5. Subjects & Categories of Records that May be Held & Information Available
6. Addendum to Employee Letter of Appointment and Declaration Form for Employees with Access to Personal Information
7. Request for Access to Record of a Private Body
8. Explanatory Note on Fees to be Charged
9. Objection to the Processing of Personal Information
10. Withdrawal of Consent to Process Personal Information
11. Request for Correction or Deletion or Destroying of Personal Information
12. Consent to Process Personal Information.
13. Consent to Newsletter / SMS / Electronic Communication

ZWARTKOP COUNTRY CLUB

Compiled June 2021