

Amberfield Retirement Village

Body Corporate

Registration number: 103/90

Protection of Personal Information Act (POPIA) Manual

Amberfield Retirement Village

Body Corporate

Index:

Section 1: Details and contact information 2

Section 2: POPIA definitions 3

Section 3: POPIA manual 4 – 8

Section 4: POPIA Community Schemes supplementary information 9 – 14

Section 5: Annexures / Forms

Amberfield Retirement Village

Body Corporate

Section 1: Details and contact information

The information officer for the Community Scheme is the Manager. Requests relating to the PAIA or POPIA should be directed to:

Amberfield Retirement Village Body Corporate

Business address: 34 Mare Street Howick 3290.

Postal address: Private Bag X010, Howick 3290

E-mail address: hr@amberfield.co.za

Website: www.amberfield.co.za

A copy of this manual is available for inspection on the website and the business address stated above.

Amberfield Retirement Village

Body Corporate

Section 2: Definitions

1. **"Community Scheme"** means Body Corporate or Home Owners' Association with a shared use of and responsibility for land / buildings as defined in the CSOS Act
2. **"Data Subject"** means a Community Scheme unit / owner / tenant. Person to whom the personal information relates
3. **"Personal Information"** means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person
4. **"Person"** means a juristic or natural person in their capacity as agent, employee, scheme executive, service provider or owner
5. **"Processing"** means any operation or activity concerning how personal information is used, shared or stored
6. **"Record"** means any recorded information, irrespective when it came into existence
7. **"Responsible Party"** means a community scheme or other person which determines the purpose and means for processing personal information
8. **"SLA"** means the Service level agreement with service providers, as amended
9. **"Visitors"** means any persons visiting the Community Scheme
10. **"POPIA"** means Protection of Personal Information Act, 2013 and its Regulations as amended
11. **"Service Provider"** means any company providing a service to the scheme
12. **"Operator"** means a party that processes information on behalf of the responsible party

Amberfield Retirement Village

Body Corporate

Section 3: POPIA Manual

This section relates to the processing of personal information in terms of POPIA

1. The responsible party may collect information from data subjects, including in the following instances:
 - 1.1. When an owner sells their unit
 - 1.2. When a new owner is registered as an owner
 - 1.3. When an owner signs a lease with a tenant
 - 1.4. When engaging with service providers
 - 1.5. For access control purposes
 - 1.6. When employing staff

2. A person or company acting as responsible party may collect the following information on data subjects:
 - 2.1. Owners/tenants, natural persons:
 - 2.1.1. Name
 - 2.1.2. ID number
 - 2.1.3. Date of birth
 - 2.1.4. Gender
 - 2.1.5. Nationality
 - 2.1.6. Telephone number
 - 2.1.7. Email address
 - 2.1.8. Physical address
 - 2.1.9. Postal address
 - 2.1.10. Biometrics (if applicable)
 - 2.1.11. Bondholder (if applicable)

Amberfield Retirement Village

Body Corporate

Section 3: POPIA Manual – continued

2.2. Owners/tenants, juristic person:

- 2.2.1. Name
- 2.2.2. Registration number
- 2.2.3. Contact person
- 2.2.4. ID number
- 2.2.5. Telephone number
- 2.2.6. Email address
- 2.2.7. Physical address
- 2.2.8. Postal address
- 2.2.9. VAT number (if applicable)
- 2.2.10. Biometrics (if applicable)
- 2.2.11. Bondholder (if applicable)
- 2.2.12. Banking Details (if Applicable)

2.3. Service providers:

- 2.3.1. Name
- 2.3.2. Registration number
- 2.3.3. Contact person
- 2.3.4. ID number
- 2.3.5. Telephone number
- 2.3.6. Email address
- 2.3.7. Physical address
- 2.3.8. Postal address
- 2.3.9. VAT number (if applicable)
- 2.3.10. Banking Details
- 2.3.11. Biometrics (if applicable)

Amberfield Retirement Village

Body Corporate

Section 3: POPIA Manual – continued

2.4. Employees:

- 2.4.1. Name
- 2.4.2. ID number
- 2.4.3. Date of birth
- 2.4.4. Gender
- 2.4.5. Nationality
- 2.4.6. Telephone number
- 2.4.7. Email address
- 2.4.8. Physical address
- 2.4.9. Postal address
- 2.4.10. Income tax number
- 2.4.11. Banking details
- 2.4.12. Biometrics (if applicable)

2.5. Visitors for access control (security data):

- 2.5.1. Name
- 2.5.2. ID number
- 2.5.3. Telephone number
- 2.5.4. Driver's license details
- 2.5.5. Vehicle registration number
- 2.5.6. Vehicle license disk details
- 2.5.7. Biometrics (if applicable)
- 2.5.8. Visual data (if applicable)

Amberfield Retirement Village Body Corporate

Section 3: POPIA Manual – continued

**3. Information may be collected for the following purposes in achieving the functions of the scheme:
Amberfield Retirement Village Body Corporate uses personal information for the following purposes**

- 3.1. Raising levies, service charges and penalties, interest, and other related charges for the scheme
- 3.2. Sending statements
- 3.3. Issuing clearance certificates
- 3.4. Legal and collection process
- 3.5. Owner / tenant correspondences
- 3.6. AGM / SGM notices
- 3.7. Staff administration and HR related work
- 3.8. Complying with other legal and regulatory requirements
- 3.9. Access control and security
- 3.10. Maintenance, garden, security, and other complex/estate related services
- 3.11. Ensuring the scheme is adequately insured

4. Information may be processed and collected in the following ways:

- 4.1. On transfer of the property from conveyance attorneys
- 4.2. Developer
- 4.3. New tenants
- 4.4. Visitors to the schemes
- 4.5. Owners / Tenants updating their details

5. Recipients of personal information:

Amberfield Retirement Village Body Corporate may share personal information with agents, service providers and others who may use this information to send the data subject information as described in section 3, point 2 above and in the fulfilment of their duties relating to the Amberfield Retirement Village Body Corporate.

6. Retention of personal information:

Amberfield Retirement Village Body Corporate may retain personal information indefinitely unless a membership ceases. In such instances the information will be kept for 5 years. When the information is no longer required, Amberfield Retirement Village Body Corporate will delete the information in a secure and safe manner.

Amberfield Retirement Village Body Corporate

Section 3: POPIA Manual – continued

7. Security measure:

Where Amberfield Retirement Village Body Corporate has appointed service providers, the service providers are required in terms of their Service Level Agreement (SLA) to ensure compliance with the POPIA. Service providers' staff are also required to be kept up to date on the POPIA requirements and may be asked to produce proof as and when required.

All information processed by service providers are to be done in adherence with the POPIA and in fulfilment with their functions.

Amberfield Retirement Village Body Corporate information officer is responsible for training and keeping the schemes staff up to date on the POPIA requirements.

Physical records pertaining personal information are safe guarded against theft and unauthorized usage. Electronic data is protected through the implementation of the necessary information technology.

Any breach in these measures will be communicated to the affected data subjects immediately.

8. Request for correction or deletion of personal information:

Data subjects may request to correct or delete their information, or object to the processing or retention of their information by completing form A and submitting the completed form to the information officer at the address shown.

Note that in terms of legislation, Amberfield Retirement Village Body Corporate is required by law to collect and retain certain information on data subjects.

Information officer: The Manager

Email address: hr@amberfield.co.za

9. Complaints in terms of POPIA:

A complaint may be lodged with the Regulator about an interference with the protection of your personal information and a breach of the POPIA. Complaints must be in writing and addressed to:

complaints.IR@justice.gov.za

10. Access to see what information is held by the scheme:

Any data subject may request details of what information is held by the scheme from the managing agent.

11. Security Camera Footage and Biometrics:

All data is stored in a secure manner and deleted when not required. Security footage may be given to the SAPS or used by the security company in apprehending criminal suspects.

Amberfield Retirement Village Body Corporate

Section 3: POPIA Manual – continued

7. Security measure:

Where Amberfield Retirement Village Body Corporate has appointed service providers, the service providers are required in terms of their Service Level Agreement (SLA) to ensure compliance with the POPIA. Service providers' staff are also required to be kept up to date on the POPIA requirements and may be asked to produce proof as and when required.

All information processed by service providers are to be done in adherence with the POPIA and in fulfilment with their functions.

Amberfield Retirement Village Body Corporate information officer is responsible for training and keeping the schemes staff up to date on the POPIA requirements.

Physical records pertaining personal information are safe guarded against theft and unauthorized usage.

Electronic data is protected through the implementation of the necessary information technology.

Any breach in these measures will be communicated to the affected data subjects immediately.

8. Request for correction or deletion of personal information:

Data subjects may request to correct or delete their information, or object to the processing or retention of their information by completing form A and submitting the completed form to the information officer at the address shown.

Note that in terms of legislation, Amberfield Retirement Village Body Corporate is required by law to collect and retain certain information on data subjects.

Information officer: The Manager

Email address: hr@amberfield.co.za

9. Complaints in terms of POPIA:

A complaint may be lodged with the Regulator about an interference with the protection of your personal information and a breach of the POPIA. Complaints must be in writing and addressed to:

complaints.IR@justice.gov.za

10. Access to see what information is held by the scheme:

Any data subject may request details of what information is held by the scheme from the managing agent.

11. Security Camera Footage and Biometrics:

All data is stored in a secure manner and deleted when not required. Security footage may be given to the SAPS or used by the security company in apprehending criminal suspects.

Amberfield Retirement Village

Body Corporate

Section 4 – POPIA Community Schemes Supplementary Information

POPIA is applicable to Community Schemes such as Sectional Title Schemes AND Home-Owner Associations and applies to all scheme executives, trustees, directors, Managing Agents as defined by the STSMA and CSOSA, and all owners / members / residents of the community scheme.

Scheme Executive Duties and Responsibilities to comply with POPIA:

Community Scheme Executives are authorised by legislation to control, manage and administer the scheme to which they have been elected as a scheme executive, usually at a meeting of the owners. They may appoint a Managing Agent to assist them regarding the administration of the scheme. Scheme Executives must be able to respond with the correct answers when owners or even visitors to a scheme, want to know what is happening to the personal information that is required to be provided by rules or by legislation. This information is used by the scheme executives for the purposes of levy collection, the arrangement of the scheme meetings and the distribution of information to members.

All community schemes should have a well laid out, legally compliant up-to-date policy about how it manages the personal information of members, residents, and visitors. The policy should include details of the type of personal information that the scheme management collects and holds, as well as how this personal information is collected and stored in a safe and responsible manner. The policy should be readily accessible and available to residents and owners and should include how and where an individual can lodge a complaint to the Information Regulator should they believe their personal information is not being correctly collected, processed or stored by the scheme.

Scheme executives must ensure that information that has been obtained from the members of a community scheme, is only used for the purposes for which it was given. If a request is made to obtain the information of one or multiple members in a scheme, scheme executives must determine if the request is legitimate, reasonable, requested in the interest of good governance of the Body Corporate, is legally allowed in terms of governing legislation of the scheme and is in the interest for the good management of the scheme. If they determine such, then they may furnish such information, especially if they are required to do so in terms of the governing legislation of the scheme.

Should any request for personal information of a member be made to the scheme executives by any party, and such request, in the opinion of the scheme executives, does not fall within the pursuit of a legitimate interest in terms of which the scheme is properly managed, then the permission of the scheme member concerned would have to be sought by the scheme executives before any personal information may be distributed. In such an instance, no information may be distributed without the member's approval and any contravention of this may result in sanctions being taken against the scheme executives, which can be onerous and punitive, as legislated by the POPIA.

The requestee of information must also acknowledge in the document that they fully realise and acknowledge the legal implications should they fail to abide by the requirements of the POPI Act, sanctions as are provided for in the POPI Act, and their responsibility and liability in dealing with the personal information of members of the community scheme that has been provided to them.

A scheme should adopt an appropriate conduct rule that covers the collection and processing of personal information.

Amberfield Retirement Village

Body Corporate

Section 4 – POPIA Community Schemes Supplementary Information – continued

Sectional Title Schemes:

Trustees of sectional title schemes are mandated by the Sectional Titles Schemes Management Act (STSMA) and its Regulations to carrying out of their duties on behalf of the Body Corporate. One of these duties is to collect the personal information of the members of the Body Corporate, and all residents residing in the scheme [Prescribed Management Rule (PMR) 27]. This information is usually stored with the Managing Agent (provided one has been appointed) but is accessible to the trustees in terms of STSMA legislation and may even be required to be made accessible to a legitimate party requesting such personal information. Such information is used for the purposes of levy collection, the arrangement of the scheme meetings, the distribution of information to members and arrear levy debt collection procedures and other legal and audit matters if required.

The actions of trustees' can be restricted by decision, by resolution of the members of the scheme taken at the AGM, but such restriction may not conflict with the STSMA which lays out the legislated duties of the trustees and their responsibilities. In terms of STSMA Section 8, Trustees have a fiduciary duty towards the Body Corporate, which means that they, in performing their duties as legislated and described in the STSMA, must always act in good faith and in the interests of the Body Corporate.

Part 6 of the Prescribed Management Rules, which are found in Annexure 1 of the STSMA regulations, deal with Administrative Management of Sectional Title Community Schemes and PMR 27 does allow a member of the Body Corporate to provide information.

PMR 27(4) reads:

On receiving a written request, the body corporate must make the records and documents referred to in this rule available for inspection by, and provide copies of them to –

- (a) A member
- (b) A registered bondholder; or
- (c) A person authorised in writing by a member or registered bondholder.

PMR 27(5) reads:

The body corporate must comply with a request for inspection or copying under this rule within 10 days.

There is no requirement in the PMR 27.4 that a reason be given for such a request, and PMR 27.5 says that the BC MUST comply with a request for inspection or copying under this rule within 10 days. However, the STSM Act in 3.1 (n) does use the words "reasonable request". If the reason is for the member to follow a PMR such as PMR 27.4, and to do so requires access to the members details in order to contact them, then that should be regarded as a "reasonable request".

Community Scheme Owners Duties and Responsibilities:

Owners/members of a scheme are required in terms of their respective governing legislation to provide accurate personal information to the scheme executives and to managing agents of a scheme when such information is requested to be provided.

Should a member find themselves in a position where their contact information has been distributed and that such distribution IS not in line with the use of the information that was agreed to or is reasonably necessary to facilitate the management of the scheme, the scheme executive, or the service provider responsible for the distribution of the information will be in transgression of POPI Act.

Amberfield Retirement Village

Body Corporate

Section 4 – POPIA Community Schemes Supplementary Information - continued

Members Rights:

Everyone has the right to be told if someone is collecting their personal information, OR if one's personal information has been made available to or accessed by an unauthorized person. Everyone has the right to access their own personal information as well as the right to require that one's personal information must be corrected or destroyed, or to object to one's personal information being processed.

The Act does not apply to personal information processed during a personal or household activity, or where the processing authority is a public body involved in national security, defence, public safety, anti-money laundering, or the Cabinet or Executive Council of the province or as part of a judicial function.

Processing of Information:

The scheme can only process Personal information in its possession:

- If it is necessary for the conclusion or performance of a contract to which the "data subject" is a party; or
- It is required by law; or
- It protects a legitimate interest of the "data subject"; or
- It is necessary to pursue your legitimate interests or the interest of a third party to whom the information is supplied.

The Service Providers as a Responsible Party will have to collect personal information directly from the owner / tenant (the "data subject"), unless:

- This information is contained in some public record or has been deliberately published by the data subject.
- Collecting the information from another source does not prejudice the subject.
- It is necessary for some public purpose; or to protect your own interests.
- Obtaining the information directly from the subject would prejudice a lawful purpose or is not reasonably possible.

The scheme can only collect personal information for a specific, explicitly defined, and lawful purpose and the subject (owner / tenant) must be aware of the purpose for which the information is being collected.

Once the personal information is no longer needed for the specific purpose, the scheme must dispose of the information in a safe and secure manner (the subject must be "de-identified"), unless the scheme needs to keep it (or is allowed to keep it) by law, or the scheme need to keep the record for a lawful purpose or in accordance with the contract between the scheme and the subject, or the subject has consented to the scheme keeping the records.

Documentation relating to personal information that has been collected, and how it has been processed, must be maintained as required by Section 14 or Section 51 of the POPIA

Any holder and keeper of personal information must to take steps to prevent the loss, damage, and unauthorised destruction of the personal information. Any scheme, service provider to the scheme, must prevent unlawful access to or unlawful processing of any personal information under their control. The scheme must identify possible risks and then establish and maintain safeguards against these identified risks.

If there has been a breach and personal information has been accessed or acquired by any unauthorised people the information officer needs to notify the Information Regulator, and the subject (if you still know who the subject was). The notification to the subject needs to provide sufficient information to allow the subject to protect themselves against the possible consequences of the personal information falling into the wrong hands.

Amberfield Retirement Village

Body Corporate

Section 4 – POPIA Community Schemes Supplementary Information – continued

The Act creates a special category of personal information called “special personal information”. This relates to religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information. Also included in this category is information relating to the alleged commission of any offence or any proceedings in respect of any offence allegedly committed and the outcome of such proceedings. One is not allowed to process this special personal information unless it is done with consent; or is necessary in law; or is done for historical, statistical or research purposes; or the information has been deliberately made public by the subject. An example of biometric register is attached.

A scheme must ensure the 8 conditions of processing information are met under Section 8 of POPIA. These are:

1. Accountability – The scheme must ensure it complies with the 8 conditions.
2. Processing limitation – Personal information must be processed lawfully, and in a responsible manner so that it does not infringe on the data subject's rights.
3. Purpose specification – Personal information must be collected for a specific purpose.
4. Further processing limitation - The further processing of the personal information by the scheme must be compatible with the purpose of collection.
5. Information quality - Responsible steps should be taken to ensure that the personal information is complete, accurate, not misleading and up to date.
6. Openness – The Scheme must maintain the documentation of the processing operations.
7. Security safeguards – The Scheme must secure the integrity and confidentiality of the personal information and take reasonable technical and operational measures to prevent unlawful access and loss.
8. Data subject participation – the data subject has the right to request the scheme to advise whether they hold personal information.

Disputes and Breaches:

If someone is alleged to be in breach of the Act, any person may submit a complaint to the Information Regulator. This complaint will be dealt with by an adjudicator. If a person is not happy with the determination of the adjudicator, they can still approach the Information Regulator for another ruling.

When a complaint is referred to the Regulator, the Regulator has certain options. He / She can

- Conduct pre-investigation.
- Act as a conciliator.
- If after investigating the complaint, the Regulator believes there is no case either because of the passing of time, the trivial subject matter of the complaint, the fact that the complaint is frivolous or vexatious or not made in good faith, or if the complainant does not have a sufficient personal interest in the matter, or where there is another internal remedy which has not yet been exhausted, or where further Action would be unnecessary or inappropriate, decide to take no action;
- Conduct a full investigation.
- Refer the complaint to the Enforcement Committee.

The Regulator also has the right to commence an investigation on their own initiative. They can also refer any complaint to another body if the Regulator believes that the complaint falls more properly within the jurisdiction of this other body. The Information Regulator has the right to summon people to appear before it and to give evidence.

The Information regulator can also enter and search any premises, conduct private interviews at any place or carry out other enquiries that the Regulator sees fit.

Amberfield Retirement Village

Body Corporate

Section 4 – POPIA Community Schemes Supplementary Information – continued

The Information Regulator is entitled to approach the judge of the High Court or a magistrate to issue a search warrant which would empower the Regulator to search, inspect, examine, operate and test any equipment used for the purposes of processing personal information on the premises. The Information Regulator also has the powers of seizure in respect of evidence or prospective evidence. The Enforcement Committee will make recommendations to the Regulator necessary or incidental to any Action that should be taken against the responsible party. The Information Regulator will make the final “judgement” on the complaint. The guilty party will be advised of their appeal rights. The enforcement notice may not require the responsible party to take any remedial action until the period for an appeal has passed, and if such appeal is lodged, until it has been determined. The Information Regulator does however have the power to enforce immediate compliance if the matter is viewed as urgent.

A guilty party has a right of appeal of to the High Court and such a party has 180 days to appeal. A subject who has suffered damages because of the responsible party failing to comply with this Act can institute a civil action to recover these damages whether there has been any intention or negligence on the part of the responsible party. This creates a strict liability on the part of the responsible party. The Act sets out a fixed number of defences that can be raised against an action for damages. These are:

- Superior force.
- Consent of the plaintiff.
- Fault on the part of the plaintiff (contributory negligence).
- That compliance was not reasonably practicable in the circumstances; or
- That the regulator had granted an exemption in respect of compliance.

If the responsible party is found to be guilty the court has the jurisdiction to award damages as compensation for patrimonial and non-patrimonial loss suffered by the subject and for aggravated damages, in a sum determined in the discretion of the court. This latter category would appear to be a type of punitive damages which is a new concept in our law. The court can also order the payment of interest on damages and costs of suit on a scale as to be determined by the court.

Any amount awarded to the subject by the court must be paid to the Information Regulator and used first to defray expenses incurred by the Information Regulator in the case. Any available balance will then be paid to the subject. The Information Regulator will therefore be able to fund some of its operation with the damages awarded by the court to a subject. Any court issuing an order of this nature must publish such an order in the Government Gazette or by such other appropriate public media announcement as the court might consider appropriate.

Loss of Information:

Should information be lost, stolen or disclosed erroneously, the scheme will:

- Notify all affected parties within a reasonable period
- Give details of how the breach occurred and what measures have been taken to retrieve it
- Give details of what information was lost, stolen, or disclosed
- Give details of measures taken to safeguard against future such events
- Report the incident to the Information Regulator

Offences, Penalties and Administrative Fines:

Sections 100 – 106 of POPIA deal with instances where parties would find themselves “guilty of an offense”. The most relevant of these are:

- Any person who hinders, obstructs, or unlawfully influences the Regulator
- A responsible party which fails to comply with an enforcement notice
- Offences by witnesses, for example, lying under oath or failing to attend hearings
- Unlawful Acts by responsible party in connection with account numbers
- Unlawful Acts by third parties in connection with account number

Amberfield Retirement Village

Body Corporate

Section 4 – POPIA Community Schemes Supplementary Information – continued

Section 107 of POPIA details which penalties apply to respective offenses. For the abovementioned offences the maximum penalties are a fine or imprisonment for a period not exceeding 10 years or to both a fine and such imprisonment. For the less serious offences, for example, hindering an official in the execution of a search and seizure warrant the maximum penalty would be a fine or imprisonment for a period not exceeding 12 months, or to both a fine and such imprisonment.

Prescribed Forms relating to the Information Regulator:

The regulations prescribe certain forms to be completed, among other things, in relation to the following matters:

1. Where a “data subject” (defined in POPI as the person to whom the personal information relates) wishes to object to the processing of personal information. A data subject may not object to information that it is required by law to give to the scheme.
2. Where a data subject wishes to request a correction be made to their personal information, or the deletion or destruction of their personal information.
3. The submission of a complaint by a data subject to the Information Regulator (form found in POPIA Regulations).

The prescribed forms accompany the regulation provide a first step towards the practical enforcement of provisions of POPI when ultimately enacted. The above represent the 3 most used forms for a community scheme.

Information Officers:

The Regulations set out the responsibilities of so-called "Information Officers". An Information Officer is responsible for ensuring compliance with POPI and PAIA. In addition to encouraging compliance with POPI and PAIA, Information Officers are required to:

- Develop, implement, monitor, and maintain a compliance framework.
- Undertake a personal information impact assessment to ensure that adequate measures and standards exist.
- Develop, monitor and maintaining an access to information manual (i.e., a PAIA manual).
- Develop internal measures and systems to process requests for information or access; and
- Conduct internal awareness sessions.

Upon implementation of POPIA, the scheme should conduct a Personal Information Impact Assessment (PIIA). This can be done by:

- Document the relationships between the scheme, and its service providers and the employees (if any). Define what each does and what information is needed
- Ask for each service providers contract and check that they have a clause in them that deals with POPIA to the satisfaction of the scheme executives. Addendums to the contracts should be signed
- Do a physical site inspection of the guardhouse and/or office. Observations should be documented
- Implement improvements where necessary e.g.: lock and key

Investigation, conciliation, and settlement of complaints:

The Regulations also provide further information in respect of the Regulator's powers and duties as regards pre-investigation, conciliation, and settlement of complaints. This is, however, primarily in respect of the prescribed forms required to be completed by the Regulator in respect of the necessary notifications to be made to the relevant parties.

The notifications include the following:

- As regards pre-investigation proceedings, if the Regulator intends to investigate any matter, the Regulator must notify the parties prior to conducting the investigation
- During the course of an investigation, the Regulator must keep the complainant, the data subject (if not the complainant) and the responsible party informed of the developments of the investigation
- If during the investigation of a complaint, the Regulator decides to act as a conciliator and convene a conciliation meeting, the Regulator must inform the data subject and responsible party implicated on the compliant form

- If it appears from a complaint, any written reply to the complaint, or during a conciliation meeting that it may be possible to secure a settlement between the parties, the Regulator may confer with the parties as required, and may hold a settlement meeting

FORM 1

OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION IN TERMS OF SECTION 11(3) OF THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013)

REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018 [Regulation 2]

Note:

1. Affidavits or other documentary evidence as applicable in support of the objection may be attached.
2. If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.
3. Complete as is applicable.

A	DETAILS OF DATA SUBJECT
Name(s) and surname/ registered name of data subject:	
Unique Identifier/ Identity Number	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number / E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname/ Registered name of responsible party:	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number/ E-mail address:	
C	REASONS FOR OBJECTION IN TERMS OF SECTION 11(1)(d) to (f) (Please provide detailed reasons for the objection)

Signed at this day of20.....

.....
Signature of data subject/designated person

FORM 2**REQUEST FOR CORRECTION OR DELETION OF PERSONAL INFORMATION OR DESTROYING OR
DELETION OF RECORD OF PERSONAL INFORMATION IN TERMS OF SECTION 24(1) OF THE
PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO.
4 OF 2013)****REGULATIONS RELATING TO THE PROTECTION OF PERSONAL INFORMATION, 2018**

[Regulation 3]

Note:

1. *Affidavits or other documentary evidence as applicable in support of the request may be attached.*
2. *If the space provided for in this Form is inadequate, submit information as an Annexure to this Form and sign each page.*
3. *Complete as is applicable.*

Mark the appropriate box with an "x".

Request for:☐

Correction or deletion of the personal information about the data subject which is in possession or under the control of the responsible party.

☐

Destroying or deletion of a record of personal information about the data subject which is in possession or under the control of the responsible party and who is no longer authorised to retain the record of information.

A	DETAILS OF THE DATA SUBJECT
Name(s) and surname / registered name of data subject:	
Unique identifier/ Identity Number:	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number/E-mail address:	
B	DETAILS OF RESPONSIBLE PARTY
Name(s) and surname / registered name of responsible party:	
Residential, postal or business address:	
	Code ()
Contact number(s):	
Fax number/ E-mail address:	
C	INFORMATION TO BE CORRECTED/DELETED/ DESTROYED/ DESTROYED
REASONS FOR *CORRECTION OR DELETION OF THE PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(a) WHICH IS IN POSSESSION OR UNDER THE CONTROL OF THE RESPONSIBLE PARTY ; and or REASONS FOR *DESTRUCTION OR DELETION OF A RECORD OF PERSONAL INFORMATION ABOUT THE DATA SUBJECT IN TERMS OF SECTION 24(1)(b) WHICH THE RESPONSIBLE PARTY IS NO LONGER AUTHORISED TO RETAIN.	
<i>(Please provide detailed reasons for the request)</i>	

Signed at this day of20.....

.....
Signature of data subject/ designated person

Scheme Biometric Register (*Special Personal Information as defined*)

In addition to the register, a written consent is required to be kept. The purpose of the register is to track consent and information held.

Abbreviations:

U – Unit
O – Owner
T - Tenant
E- Employee
VS – Contractor

Scheme Biometrics Register				
OCCUPIERS			NON-OCCUPIERS	
Scheme Unit No.	Owner Code	Tenant Code	Employee Code	Contractor code
1	U1-O1 U1-O2	U1-T1	U1-E1 U1-E2	U1-VS1
2	U2-O1 U2-O2	U2-T1 U2-T2	U2-E1 U2-E2	U2-VS2
3	U3-O1 U3-O2	U3-T1 U3-T2	U3-E1 U3-E2	U3-VS3

**Addendum to Service Provider Contract
Entered into by Amberfield Body Corporate
(Registration number:)**

**hereinafter referred to as "the Community Scheme"
and**

(service provider name)

1. Definitions

In this agreement, unless the context otherwise indicates —

"Community Scheme" means Body Corporate or Home Owners Association with a shared use of and responsibility for land / buildings as defined in the Community Schemes Ombud Service Act, 2011

"Data Subject" means a Community Scheme / unit owner / tenant / visitors / other Service Providers. Person to whom the personal information relates "Information Officer" the principle of the Service Provider, or as appointed by it, whose function is defined under the Protection of Personal Information Act, 2013

"Operator" means a party that processes information on behalf of the responsible party

"Personal Information" means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person

"POPIA" means Protection of Personal Information Act, 2013 and its Regulations as amended

"Processing" means any operation or activity concerning how personal information is used, shared or stored

"Responsible Party" means a Community Scheme or other person which determines the purpose and means for processing personal information

"SLA" means the Service Level Agreement / contract with service providers, as amended

"Visitor" means any persons visiting the Community Scheme

"Service Provider" means any company or individual providing a service to the scheme

"Services" mean the services provided by the Service Provider to the Community Scheme and as defined in the Service Level Agreement / contract

2. Context

The purpose of this addendum is to clarify the Service Provider's responsibilities and obligations in terms of the Protection of Personal Information Act, 2013 (POPIA) when dealing with the Personal Information of any Data Subjects as described in the definitions above and in the POPIA.

The Service Provider warrants that it has sufficient knowledge, systems and expertise in all aspects of the services it provides, and in particular for the provisions of POPIA. The Service Provider records that its own Information Officer and its staff have been sufficiently trained on POPIA.

The Service Provider will act as both Responsible Party and Operator to the Scheme. It is responsible for its own methods of collection, processing and destruction of Personal Information.

It is understood that the purpose of POPIA is to protect the right to privacy under the constitution of South Africa.

It is not meant to hinder the function of the Scheme, or the services offered by the Service Provider.

3. Duration

Notwithstanding the date of signature, this addendum shall continue for as long as the scheme enlists the services of the Service Provider.

4. Confidentially

The Service Provider, its employees and / or sub-contractor (Operator), confirms that all information belonging to the Scheme will be kept strictly confidential.

5. Collection of Information

5.1. The Service Provider may collect information for the sole purpose of performing its services to the Scheme. The Service Provider may collect information through a secure means of its choice, be it manually, by phone or electronic means. When collecting such information, it shall seek the permission of the Data Subject (in need) and notify them of its intended use.

5.2. Any information collected when performing its services will belong to the Scheme and not to the Service Provider.

6. Processing of Information

6.1. The Scheme hereby authorises the processing of information under Section 20 of POPIA by the Service Provider in the fulfilment of its services to the Scheme.

6.2. The Service Provider will process only necessary information.

6.3. The Service Provider will have the sole discretion on what system/s and processes to use, both from an operational and Information Technology (IT) perspective (unless otherwise stated in its SLA).

7. Request for Information

7.1. Requests may only be made if reasonable and in line with the relevant legislation pertaining to the Scheme. No information will be divulged to a third party without the written consent of the Scheme Executives and Data Subject (if needed).

7.2. A Data Subject may at any time-to-time request details of the information held by the Service Provider and may request amendment and / or deletion (if applicable).

7.3. Should the Scheme terminate the services of the Service Provider, it shall hand over all information to the Scheme Executives or as directed by them.

8. Destruction of Information

8.1. Information required for financial records will be kept for 5 years. Permanent records (e.g: building plans; financial statements) will be kept indefinitely. Information not required will be destroyed and/or deleted. A certificate of destruction, if requested, must be produced in the case of hard copies being destroyed.

8.2. The Service Provider may be held liable for loss of, damage to or unauthorised destruction of personal information. Such replacement cost would be for the Service Provider.

8.3. A Data Subject may request the deletion/destruction of Personal Information held by the Service Provider if such information is no longer required to fulfil the function of the scheme.

9. Information Technology

The Service Providers confirms that it has sufficient protection against viruses and theft of data.

10. Physical Security Measures

The Service Provider confirms that hard copies of Personal Information are kept under lock and key.

11. Breach of Information

Should a breach of information occur, accidentally or otherwise, the Service Provider undertakes to:

- a. Report the breach to the Scheme Executives immediately
- b. Notify the affected Data Subject of what information has been lost/divulged *(for the Data Subject to take appropriate steps to protect themselves)*
- c. Notify the affected Data Subject what action has been taken to rectify the breach

12. Indemnity

The Service Provider hereby indemnifies the Scheme Executives against any loss, fine or claim as a direct result of the gross negligence when handling information belonging to the scheme. Any loss as a result thereof will be for the account of the Service Provider.

Scheme Executive

Scheme Executive

Thus done and signed at _____ this _____ day of _____ 20____

For and on behalf of Service Provider

Who warrants that he/she is duly authorised hereto

REQUEST FOR INFORMATION

Owners requesting information from the scheme are requested to complete this form

A. Particulars of person requesting information

- (a) The particulars of the person who requests access to the information must be given below.

(b) Proof of the capacity in which the request is made, if applicable, must be attached.

Full names and surname:

Identity number:

--	--	--	--	--	--	--	--	--	--	--	--	--	--

Postal address:

.....

Telephone number: (.....) Fax number: (.....)

E-mail address:

.....

Capacity:

.....

B. Particulars of information requested

- (a) Provide full particulars of the information you are requesting in terms of the schemes governance documentation. Please cite the relevant clause.

(b) If the provided space is inadequate, please continue on a separate folio and attach it to this form. The requester must sign all the additional folios.

1. Description of information requested:

.....

.....

.....

.....

3. Full reason why the information is requested:

.....

.....

.....

.....

.....

.....
.....
.....

C. Fees

You will be notified of the amount, should a fee be applicable. Not all requests will attract a fee depending on time and resources required.

D. Format of information

1. If the record is in written or printed form:					
	Copy of info		Inspection of info		

2. If info consists of visual images - (this includes photographs, slides, video recordings, computer-generated images, sketches, etc.):					
	View the images		Copy of the images		Transcription of the images

3. If info is held on computer or in an electronic or machine-readable form:					
	printed copy of info		printed copy of info derived from the record		copy in computer readable form (flash drive /compact disc)

E. Notice of decision regarding request for access

You will be notified in writing whether your request for information has been granted/denied. Should you not be happy with the decision, it is your right to approach the Community Schemes Ombudsman.

Signed at this day of year

.....
SIGNATURE OF REQUESTER