



Protection of Personal Information Act No. 4 of 2013



## Table of contents

1.	Introduction	2
2.	Definitions	2
3.	Purpose	2
4.	Application	3
5.	Rights of data subjects	3
6.	General guiding principles	4
7.	Information officer	6
8.	Personal information collected	6
9.	How personal information is used	6
10.	Disclosure of personal information	7
11.	Specific duties and responsibilities	7
12.	POPI audit	10
13.	Complaints procedure	11
14.	Disciplinary action	11
15.	Amendments to and review of this policy	11
	Annexure A – Personal information request form	12
	Annexure B – POPI complaint form	13
	Annexure C – Particulars relating to company data subjects	14
	Annexure D – POPI notice and consent form	16
	Annexure E – Sample consent and confidentiality clauses to be included in company employment agreement	17
	Annexure F – Sample service level agreement confidentiality clause	18
	Annexure G – Data processing agreement for operators	19

## POPI Policy

### 1. Introduction

- 1.1 POPI's purpose is to, *inter alia*, give effect to the constitutional right to privacy by safeguarding Personal Information when processed by a Responsible Party, subject to justifiable limitations aimed at balancing the right to privacy against other rights (particularly the right of access to information) and protecting important interests, including the free flow of information within South Africa and across international borders.
- 1.2 The Company is a real estate investment trust listed on the Johannesburg Stock Exchange and is a Responsible party under POPI in that the Company determines the purpose of and means for Processing Personal Information. As such, POPI requires the Company to inform the Company's Data Subjects as to the manner in which their Personal Information is collected, used, disclosed and destroyed.
- 1.3 The Company is committed to effectively managing Personal information in accordance with the provisions of POPI.

### 2. Definitions

- 2.1 For the purpose of this policy, unless the context indicates otherwise, the following words and expressions shall bear the following meanings:
  - 2.1.1 "**Company**" means Equites Property Fund Limited;
  - 2.1.2 "**Company's Data Subjects**" means the Company's existing, prospective and future tenants, suppliers / vendors, shareholders, brokers, analysts and employees / interns / learners, and "**Company Data Subject**" shall mean a reference to any one of them as the context may require;
  - 2.1.3 "**PAIA**" means the Promotion of Access to Information Act No. 2 of 2000;
  - 2.1.4 "**Policy**" means this protection of personal information policy;
  - 2.1.5 "**POPI**" means the Protection of Personal Information Act No. 4 of 2013, as amended;
- 2.2 Capitalised terms not otherwise defined herein shall have the meaning ascribed thereto in POPI.

### 3. Purpose

- 3.1 The purpose of this Policy is to protect the Company from the compliance risks associated with the protection of Personal Information, which includes:
  - 3.1.1 breaches of confidentiality where Personal Information of Data Subjects has been collected or disclosed inappropriately;
  - 3.1.2 failure to allow Data Subjects to choose how and for what purpose the Company collects and uses Personal Information relating to them;
  - 3.1.3 reputational damage associated with a breach of the provisions of POPI.
- 3.2 This Policy demonstrates the Company's commitment to protecting the privacy rights of Data Subjects:
  - 3.2.1 through stating the manner in which the Company shall comply with the provisions of POPI and related best practices;
  - 3.2.2 by cultivating an organisational culture that recognises privacy as a valuable constitutional right;
  - 3.2.3 by developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of Personal Information;
  - 3.2.4 by creating business practices and policies that will provide reasonable assurance that the privacy rights of Data Subjects are protected and balanced with the legitimate business needs of the Company;
  - 3.2.5 by assigning specific duties and responsibilities to the Information Officer (and his/her deputy(ies), where applicable) in order to protect the interests of the Company and Data Subjects;
  - 3.2.6 by raising awareness through training and providing guidance to individuals who process Personal Information within or on behalf of the Company so that such individuals can consistently comply with the provisions of POPI and this Policy.

## POPI Policy continued

### 4. Application

- 4.1 This Policy and its guiding principles apply to:
- 4.1.1 the Company's governing body;
  - 4.1.2 all subsidiaries of the Company;
  - 4.1.3 all employees of the Company; and
  - 4.1.4 all contractors, suppliers and other persons acting on behalf of the Company.
- 4.2 This Policy's guiding principles find application in all situations and must be read in conjunction with POPI, as well as the provisions of PAIA.
- 4.3 The legal duty to comply with the provisions of POPI is activated in any situation where there is Processing of Personal Information entered into a Record by or for a Responsible Person who is domiciled in South Africa.
- 4.4 POPI does not apply in situations where the Processing of Personal Information is concluded in the course of purely personal or household activities or where the Personal Information has been Deldentified.

### 5. Rights of data subjects

Where appropriate, the Company will ensure that the Company Data Subjects are made aware of the rights listed below and conferred on them as Data Subjects.

#### 5.1 Right to Access Personal Information

- 5.1.1 The Company recognises that a Data Subject has the right to establish whether the Company holds Personal Information related to him/her/it and has the right to request access to that Personal Information.
- 5.1.2 When requesting such access, Data Subjects are requested to make use of the form annexed hereto as **Annexure A**. For the avoidance of doubt it is recorded that, despite **Annexure A** providing for a Data Subject to request that the Record of his/her/its Personal Information be destroyed, such Record can only be destroyed where the Company is no longer authorised to retain it in terms of section 14 of POPI.

#### 5.2 Right to have Personal Information Corrected or Deleted

The Data Subject has the right to request, where necessary, that his/her/its Personal Information be corrected or, where the Company is no longer authorised to retain the Personal Information, deleted.

#### 5.3 Right to Object to Processing of Personal Information

- 5.3.1 The Data Subject has the right to, on reasonable grounds, to object to the Processing of his/her/its Personal Information.
- 5.3.2 In such circumstances, the Company shall give due consideration to the request and the provisions of POPI and the Company may:
- 5.3.2.1 cease to use or disclose the Data Subject's Personal Information; and/or
  - 5.3.2.2 subject to any statutory and/or contractual recordkeeping requirements, approve the destruction of the Personal Information.

#### 5.4 Right to Object to Direct Marketing

The Data Subject has the right to object to the Processing of his/her/its Personal Information for purposes of direct marketing by means of unsolicited electronic communications.

#### 5.5 Right to Complain

- 5.5.1 The Data Subject has the right to complain to the Company, should he/she/it be of the opinion that any of his/her/its rights under POPI have been infringed. For such purposes, Data Subjects are encouraged to make use of the POPI complaint form annexed hereto as **Annexure B**.

## POPI Policy continued

- 5.5.2 The Company undertakes to investigate all POPI-related complaints in accordance with the procedure set out in clause 13 below.
- 5.5.3 Should the Data Subject not be satisfied with the Company's response, he/she/it has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPI and to institute civil proceedings regarding the alleged noncompliance with the protection of his/her/its Personal Information.

### 5.6 Right to be Informed

The Data Subject has the right to be notified:

- 5.6.1 that his/her/its Personal information is being collected by the Company;
- 5.6.2 in any situation where the Company has reasonable grounds to believe that his/her/its Personal Information has been accessed or acquired by an unauthorised person.

## 6. General guiding principles

This Policy's guiding principles find application in all situations and must be read in conjunction with POPI, as well as the provisions of PAIA.

### 6.1 Accountability

- 6.1.1 Failure to comply with POPI could potentially damage the Company's reputation and/or expose it to administrative fines and civil claims for damages. Individuals found guilty of violating POPI could also be fined or imprisoned for prescribed periods. The protection of Personal Information is accordingly the responsibility of every stakeholder in the Company.
- 6.1.2 The Company will ensure that the provisions of POPI and the guiding principles outlined in this Policy are complied with through the encouragement of POPI-compliant behaviour. Where individuals, through intentional or negligent actions and/or omissions, fail to comply with the principles and responsibilities outlined in this Policy, the Company will make appropriate sanctions against such individuals, which may include disciplinary action.

### 6.2 Processing Limitation

- 6.2.1 The Company will ensure that Personal Information under its control is Processed:
- 6.2.1.1 in a fair, lawful and nonexcessive manner; and
- 6.2.1.2 only with the informed consent of the Data Subject; and
- 6.2.1.3 only for a specifically defined purpose.
- 6.2.2 The defined purposes for which the Company Processes each of the Company Data Subjects' Personal Information are listed in **Annexure C**.
- 6.2.3 The Company will inform the Data Subject of the reasons for collecting his/her/its Personal Information and take reasonable steps to obtain written consent prior to Processing Personal Information.
- 6.2.4 The Company will not, under any circumstances, distribute or share Personal Information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.
- 6.2.5 Where applicable, the Data Subject must be informed of the possibility that their Personal Information will be shared with other aspects of the Company's business and be provided with reasons for doing so.
- 6.2.6 A template notice and consent form is annexed hereto as **Annexure D**.

### 6.3 Purpose Specification

- 6.3.1 All of the Company's business units and operations must be informed by the principle of transparency and accountability.
- 6.3.2 The Company will Process Personal Information only for specific, explicitly defined and legitimate purposes, as set out in **Annexure C** hereto.

## POPI Policy continued

### 6.4 Further Processing Limitation

6.4.1 Personal Information will not be Processed for a secondary purpose unless that Processing is compatible with the original purpose. Accordingly, where the Company seeks to Process Personal Information it holds for a purpose other than the purpose(s) set out in **Annexure C** hereto, and where this secondary purpose is not compatible with the original purpose, the Company will first obtain consent in relation to such secondary purpose from the Data Subject.

### 6.5 Information Quality

6.5.1 The Company will take reasonable steps to ensure that all Personal Information collected is complete, accurate and not misleading.

6.5.2 Where Personal Information is collected/received from third parties, the Company will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information with the Data Subject or by way of independent sources.

### 6.6 Open Communication

6.6.1 The Company will take reasonable steps to ensure that Data Subjects are notified:

6.6.1.1 that their Personal Information is being collected; and

6.6.1.2 as to the purpose for which Personal Information is collected and Processed.

6.6.2 Data Subjects will be able to communicate with the Company's Information Officer by email in order to:

6.6.2.1 enquire whether the Company holds his/her/its Personal Information; and/or

6.6.2.2 request access to his/her/its Personal Information; and/or

6.6.2.3 request the Company to update or correct his/her/its Personal Information; and/or

6.6.2.4 make a complaint concerning the Processing of Personal Information.

### 6.7 Security Safeguards

6.7.1 The Company will manage the security of its filing systems to ensure that Personal Information is adequately protected. In this regard, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification or destruction.

6.7.2 The Company will continuously review its security controls, which will include regular testing of protocols and measures put in place to combat cyberattacks on the Company's information technology network.

6.7.3 The Company will ensure that all paper and electronic records containing Data Subjects' Personal Information are securely stored and made accessible only to authorised individuals.

6.7.4 All new employees will be required to sign employment agreements containing contractual terms for the use and storage of employees' Personal Information, as well as a confidentiality clause to reduce the risk of unauthorised disclosures of Personal Information for which the Company is responsible. All existing employees will, following the requisite consultation process, be required to sign an addendum to their employment agreement containing the relevant consent and confidentiality clauses, samples of which can be found in **Annexure E** hereto.

6.7.5 The Company's thirdparty service providers will be required to enter into service level agreements with the Company where both parties pledge their mutual commitment to POPI. An example of a confidentiality clause for inclusion in the Company's service level agreements can be found under **Annexure F**.

6.7.6 Those third-party service providers, defined as "Operators" in terms of POPI, who process Personal Information for the Company, the "Responsible Party", in terms of a contract or mandate will be required to enter into a data processing agreement with the Company. An example of a data processing agreement can be found under **Annexure G**.

## POPI Policy continued

### 6.8 Data Subject Participation

- 6.8.1 A Data Subject may request the correction or deletion of his/her/its Personal Information held by the Company by way of submitting the duly completed Personal Information Request Form contained in **Annexure A** hereto.
- 6.8.2 Where applicable, the Company will include a link to unsubscribe from any of its electronic newsletters or electronically transmitted marketing content.

### 7. Information officer

- 7.1 The Company will appoint an Information Officer and, where necessary, a deputy information officer. The Information Officer (and his/her deputy(ies), where applicable) shall be responsible for ensuring compliance with POPI.
- 7.2 Once appointed, the Company will register the Information Officer with the South African Information Regulator established under POPI prior to performing his/her duties.
- 7.3 The Information Officer (and his/her deputy(ies), where applicable) shall be reappointed or replaced annually.
- 7.4 Where no Information Officer is appointed, the head of the Company will assume the role of the Information Officer.
- 7.5 The Information Officer's contact details shall be available on the Company's website.

### 8. Personal information collected

- 8.1 The Company collects and Processes Personal information pertaining to Company Data Subjects. The type of information collected depends on which Company Data Subject the information relates to and the purpose for which such information is required by the Company, as set out in **Annexure C** hereto. The information will be collected and Processed only for the purposes set out in **Annexure C**.
- 8.2 The Company also collects and Processes Personal Information for marketing purposes.
- 8.3 The Company has, or undertakes to procure, agreements with all of its third-party service providers (including operators) and suppliers / vendors to ensure that there is a mutual understanding with regard to the protection of Company Data Subjects' Personal Information. Moreover, the Company's local third-party service providers (including operators) and suppliers / vendors are also subject to POPI.

### 9. How personal information is used

- 9.1 Company Data Subjects' Personal Information will only be used for the purpose(s) stated in **Annexure C**.
- 9.2 POPI provides that Personal Information may only be Processed if:
- 9.2.1 the Data Subject consents to the Processing of his/her/its Personal Information;
- 9.2.2 the Processing in question is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party;
- 9.2.3 the Processing complies with an obligation imposed by law on the Responsible Party;
- 9.2.4 the Processing protects a legitimate interest of the Data Subject; or
- 9.2.5 the Processing is necessary for pursuing the legitimate interests of the Responsible Party or of a third party to whom the information is supplied.
- 9.3 In satisfaction of the conditions set out above:
- 9.3.1 where required, Company Data Subjects shall be requested to submit duly completed consent forms in the form annexed hereto as **Annexure D**;
- 9.3.2 it is recorded that the Company only requests Personal Information which is required from Company Data Subjects in order to comply with the Company's obligations and that the Processing thereof is necessary to pursue and protect the legitimate interests of the Company, the Company Data Subjects and the third parties to whom Personal Information is supplied.

## POPI Policy continued

### 10. Disclosure of personal information

- 10.1 The Company may disclose Company Data Subjects' Personal Information to any of its subsidiaries, joint venture companies and/or approved supplier or thirdparty service providers (including operators) whose products or services require access to such Personal Information. The company has agreements in place with such suppliers and service providers to ensure compliance with confidentiality and privacy undertakings.
- 10.2 The Company may share Company Data Subjects' Personal Information with, and obtain information about Company Data Subjects from, third parties (including operators) for the purposes set out in **Annexure C**.
- 10.3 The Company may disclose Company Data Subjects' Personal Information where it has a duty or right to disclose such information in terms of applicable laws or where it may be deemed necessary and reasonable in order to protect the Company's rights.

### 11. Specific duties and responsibilities

#### 11.1 Governing Body

- 11.1.1 The Company's governing body cannot delegate its accountability and is ultimately answerable in respect of the Company's ongoing compliance with its obligations under POPI, however the governing body may delegate some of its responsibilities under POPI to management and other capable individuals within the Company.
- 11.1.2 The governing body is responsible for ensuring that:
- 11.1.2.1 the Company appoints an Information Officer and, where necessary, a deputy Information Officer/s;
  - 11.1.2.2 all persons responsible for the Processing of Personal Information on behalf of the Company:
    - 11.1.2.2.1 are appropriately trained and supervised to do so;
    - 11.1.2.2.2 understand that they are contractually obligated to protect the Personal Information they access; and
    - 11.1.2.2.3 are aware that a wilful or negligent breach of this Policy may lead to disciplinary action against them;
  - 11.1.2.3 Data Subjects wishing to enquire about their Personal Information are made aware of the procedure that must be followed;
  - 11.1.2.4 the scheduling of a periodic POPI audit in order to accurately assess and review the ways in which the Company collects, holds, uses, shares, discloses, destroys and Processes Personal Information.

#### 11.2 Information Officer

- 11.2.1 The Company's Information Officer is responsible for:
- 11.2.1.1 taking steps to ensure the Company's compliance with the provisions of POPI;
  - 11.2.1.2 updating the governing body regarding the Company's responsibilities under and pursuant to the provisions of POPI;
  - 11.2.1.3 regularly analysing privacy regulations and aligning them with the Company's internal procedures, including reviewing and updating this Policy where appropriate;
  - 11.2.1.4 ensuring that POPI audits are conducted on a regular basis;
  - 11.2.1.5 ensuring that the Company provides convenient processes for Data Subjects wishing to update their Personal Information or submit POPIrelated complaints to the Company;
  - 11.2.1.6 reviewing and approving any agreements concluded with operators, employees and other third parties which may have an impact in the Personal Information held by the Company, including overseeing the amendment of the Company's employment agreements and service level and other agreements, to the extent necessary so as to be consistent with this Policy and the provisions of POPI;
  - 11.2.1.7 ensuring that employees and other persons acting on behalf of the Company are aware of the risks associated with Processing Personal Information and that they remain informed about the Company's obligations under POPI;

## POPI Policy continued

- 11.2.1.8 organising and overseeing awareness training of employees and other individuals involved in the Processing of Personal Information on behalf of the Company;
- 11.2.1.9 addressing the Company's employees' POPI-related questions and/or concerns;
- 11.2.1.10 addressing all POPI-related requests and complaints submitted in accordance with the provisions of this Policy to the Company;
- 11.2.1.11 cooperating and working with the Information Regulator in relation to any ongoing investigations in respect of the Company and, where appropriate, any other matter.
- 11.2.2 The deputy Information Officer/s is responsible for assisting the Information officer in the performance of his/her duties set out above and elsewhere in this Policy and in POPI.
- 11.3 **IT Manager**
- The Company's IT manager is responsible for:
- 11.3.1 ensuring that:
- 11.3.1.1 the Company's IT infrastructure, filing systems and any other devices used for Processing Personal Information meet acceptable security standards;
- 11.3.1.2 all electronically stored Personal Information is:
- 11.3.1.2.1 kept only on designated drives and servers and uploaded only to approved cloud computing services;
- 11.3.1.2.2 backed up and tested on a regular basis;
- 11.3.1.3 servers containing Personal Information are sited in a secure location;
- 11.3.1.4 Personal Information transferred electronically is encrypted;
- 11.3.1.5 all servers and computers containing Personal information are protected by a firewall and the latest security software;
- 11.3.2 performing:
- 11.3.2.1 regular IT audits to ensure that the security of the Company's hardware and software systems are functioning properly and to verify whether electronically stored Personal Information has been accessed or acquired by any unauthorised person;
- 11.3.2.2 a due diligence review prior to contracting with operators or thirdparty service providers to Process Personal Information on the Company's behalf.
- 11.4 **Marketing and Communications Manager**
- The Company's marketing and communications manager is responsible for:
- 11.4.1 approving and maintaining statements and disclaimers in relation to the protection of Personal Information that are displayed on the Company's website, including those attached to communications such as emails and electronic newsletters;
- 11.4.2 addressing any Personal Information protection queries from journalists or media publications or outlets;
- 11.4.3 where necessary, working with persons acting on behalf of the Company to ensure that any outsourced marketing initiatives comply with the provisions of this Policy and POPI.
- 11.5 **Employees and Other Persons acting on behalf of the Company**
- 11.5.1 Employees and other persons acting on behalf of the Company (collectively "**Authorised Persons**") will, during the course of the performance of their roles within the Company, gain access to and become acquainted with Data Subjects' Personal Information. Authorised Persons are required to treat such Personal Information as a confidential business asset and to respect the privacy of all Data Subjects.

## POPI Policy continued

- 11.5.2 Authorised Persons may not directly or indirectly utilise, disclose or make public in any manner to any person or third party, either within the Company or externally, any Personal Information unless such information is already publicly known or the disclosure is necessary in order for the Authorised Person to perform his/her duties.
- 11.5.3 Authorised Persons must request assistance from their line manager or the Company's Information Officer if they are unsure about any aspect related to the protection of a Data Subject's Personal Information.
- 11.5.4 Authorised Persons will only Process Personal Information where:
- 11.5.4.1 the Data Subject or the Data Subject's duly authorised representative consents to the Processing;
  - 11.5.4.2 the Processing is necessary to carry out actions for the conclusion or performance of a contract to which the Data Subject is party;
  - 11.5.4.3 the Processing is consistent with an obligation imposed by law on the Responsible Party;
  - 11.5.4.4 the Processing protects a legitimate interest of the Data Subject;
  - 11.5.4.5 the Processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom the information is supplied.
- 11.5.5 Moreover, Personal Information will only be Processed where the Data Subject in question:
- 11.5.5.1 clearly understands why and for what purpose his/her/its Personal Information is being collected; and
  - 11.5.5.2 one or more of the grounds under POPI to justify the processing of Personal Information has been satisfied.
- 11.5.6 Prior to Processing any Personal Information, Authorised Persons must take reasonable steps to obtain specific informed consent from the Data Subject in terms of which permission is given for the Processing of Personal Information. For purposes hereof:
- 11.5.6.1 "**informed consent**" shall entail the Data Subject clearly understanding the purpose for which his/her/its Personal Information is needed and who it will be shared with;
  - 11.5.6.2 informed consent to Process Personal Information must be obtained directly from the Data Subject except where:
    - 11.5.6.2.1 the personal Information has been made public; or
    - 11.5.6.2.2 valid informed consent has been given to a third party; or
    - 11.5.6.2.3 the information is necessary for effective law enforcement;
- 11.5.7 Authorised Persons will under no circumstances:
- 11.5.7.1 Process or have access to personal information where such Processing or access is not required to perform their workrelated tasks or duties;
  - 11.5.7.2 save copies of Personal information directly to their own private computers, laptops or other mobile devices. All Personal Information must be accessed and updated from the Company's central database or a dedicated server;
  - 11.5.7.3 share Personal Information informally. Where access to Personal Information is required, it may be requested from the relevant line manager or the Information Officer;
  - 11.5.7.4 transfer Personal information outside of South Africa without the express permission of the Information Officer.
- 11.5.8 Authorised Persons are responsible for:
- 11.5.8.1 keeping all Personal Information they come into contact with secure by taking sensible precautions and following the guidelines outlined herein;
  - 11.5.8.2 ensuring that:
    - 11.5.8.2.1 Personal Information is held in as few places as possible. No unnecessary additional records, filing systems or data sets should be created;

## POPI Policy continued

- 11.5.8.2.2 Personal Information is encrypted prior to sharing it electronically, if necessary with the assistance of the IT manager;
- 11.5.8.2.3 all computers, laptops, mobile devices, flash drives, smartphones that other devices which store Personal Information are passwordprotected and never left unattended. Passwords must be changed regularly and must not be shared with unauthorised persons;
- 11.5.8.2.4 computer screens and other devices are switched off or locked when not in use;
- 11.5.8.2.5 where Personal Information is stored on removable storage devices such as external drives, CDs, DVDs, flash drives and other such devices, these devices are securely locked away when not in use;
- 11.5.8.2.6 where Personal Information is stored on paper, such hard copy records must be kept in a secure place where unauthorised people cannot access it;
- 11.5.8.2.7 where Personal Information has been printed, the paper printouts are not left unattended where unauthorised individuals could see or copy them;
- 11.5.8.3 taking reasonable steps to ensure that Personal Information:
  - 11.5.8.3.1 is kept accurate and uptodate, for instance by confirming a Data Subject's contact details when communicating with them;
  - 11.5.8.3.2 which is inaccurate or not uptodate, inform the relevant line manager or Information Officer of the requisite amendments to be made; and
  - 11.5.8.3.3 is stored only for so long as it is needed or required in terms of the purpose for which it was originally collected. Where Personal Information is no longer required, authorisation must first be obtained from the relevant line manager or Information Officer before deleting or disposing of the Personal information in the appropriate manner; and
- 11.5.8.4 undergoing POPI awareness training from time to time.
- 11.5.9 Where an Authorised Person becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction or the unsanctioned disclosure of Personal Information, he/she must immediately report such event or suspicion to the Information Officer or the deputy Information Officer/s.

## 12. POPI audit

- 12.1 The Company's Information Officer will schedule periodic POPI audits in order to:
  - 12.1.1 identify the processes used to collect, record, store, disseminate and destroy Personal Information;
  - 12.1.2 determine the flow of Personal Information throughout the Company;
  - 12.1.3 where necessary, redefine the purpose for gathering and Processing Personal Information;
  - 12.1.4 ensure that the processing parameters are still adequately limited;
  - 12.1.5 ensure that new Data Subjects are made aware of the Processing of their Personal Information;
  - 12.1.6 reestablish the rationale for any further Processing where information is received via a third party;
  - 12.1.7 verify the quality and security of Personal Information;
  - 12.1.8 monitor the extent of compliance with POPI and this Policy;
  - 12.1.9 monitor operators' compliance to data processing agreements; and
  - 12.1.10 monitor the effectiveness of internal controls established to manage the Company's POPIrelated compliance risk.
- 12.2 In performing the POPI audit, the Information Officer will liaise with line managers in order to identify areas within the Company's operation that are most vulnerable or susceptible to unlawful Processing of Personal Information.
- 12.3 The Information Officer (and his/her deputy(ies), where applicable) will have direct access to, and have demonstrable support from, line managers and the Company's governing body in performing his/her duties.

## POPI Policy continued

### 13. Complaints procedure

- 13.1 Data Subjects have the right to complain in instances where any of their rights under POPI have been infringed. The Company undertakes to investigate all POPIrelated complaints in accordance with the procedure set out hereunder.
- 13.2 POPIrelated complaints must be submitted to the Company's Information Officer in writing using the complaint form annexed hereto as **Annexure B**.
- 13.3 The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 7 days of receipt thereof.
- 13.4 The Information Officer:
- 13.4.1 will consider the complaint and endeavour to resolve the subject matter of the complaint in a fair manner and in accordance with the principles outlined in POPI; and
- 13.4.2 must determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the Company's Data Subjects.
- 13.5 The Information Officer will revert to the complainant with a proposed solution, together with the option to escalate the complaint to the Company's governing body, within 14 days of receipt of the complaint. The Information Officer will provide reasons for any decisions taken and will communicate any anticipated deviation from the timelines set out herein to the complainant.
- 13.6 The Information Officer's response to the complainant may comprise any of:
- 13.6.1 a suggested remedy for the complaint;
- 13.6.2 a dismissal of the complaint and the reason as to why it was dismissed;
- 13.6.3 if applicable, an explanation of what went wrong and the nature of the corrective measures taken.
- 13.7 Where the complainant is not satisfied with the Information Officer's response to the complaint, the complainant may submit a complaint to the Information Regulator.
- 13.8 Where the Information Officer has reason to believe that the Personal Information of Data Subjects has been accessed or acquired by an unauthorised person, the Information Officer will consult with the Company's governing body, whereafter the affected Data Subject(s) and the Information Regulator will be informed of the breach.
- 13.9 The Information Officer will review the complaints procedure periodically in order to assess the effectiveness of the procedure and improve on the procedure where necessary.

### 14. Disciplinary action

- 14.1 Where a POPIrelated complaint or an investigation into an alleged infringement of POPI has been finalised, the Company may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being involved in any noncompliant activity outlined within this Policy and POPI.
- 14.2 Where the act/omission of such employee was as a result of ignorance or poor work performance, the Company will provide further training to the employee.
- 14.3 Any wilful negligence or mismanagement of Personal Information on the part of an employee will be considered a serious form of misconduct for which the Company may take appropriate action against the employee, including disciplinary procedures and dismissal proceedings.
- 14.4 Where applicable, the Company must, in addition to taking such disciplinary steps against the employee in question, refer the misconduct to the appropriate law enforcement agency for criminal investigation.

### 15. Amendments to and review of this policy

This Policy may be reviewed and/or amended on an *ad hoc* basis and where the Policy is amended, the amended document will be made available on the Company's website.

## POPI Policy continued

### Annexure A – Personal information request form

#### Personal information request form

Please submit completed form to the company's information officer

Please be aware that we may require you to provide proof of identification prior to processing your request for providing copies of the information requested

A. Particulars of data subject	
Name & surname	
Identity number	
Postal address	
Contact number	
Email address	
B. Request	
I request the Company to	
(i) inform me whether it holds any of my personal information;	<input type="checkbox"/>
(ii) provide me with a record or description of my personal information;	<input type="checkbox"/>
(iii) correct or update my personal information;	<input type="checkbox"/>
(iv) destroy or delete a record of my personal information.	<input type="checkbox"/>
C. Instructions	
D. Signature	
Signature	
Date	

## POPI Policy continued

### Annexure B – POPI complaint form

#### POPI complaint form

Please submit completed form to the company's information officer

Where we are unable to resolve your complaint to your satisfaction, you have the right to submit a complaint to the information regulator (<https://www.Justice.Gov.Za/inforeg>)

A. Particulars of complainant	
Name & surname	
Postal address	
Identity number	
Contact number	
Email address	
B. Details of complaint	
C. Desired outcome	
D. Signature	
Signature	
Date	

## POPI Policy continued

### Annexure C – Particulars relating to company data subjects

1. The table below sets out the Company Data Subjects, the categories of Personal Information collected / Processed from or in relation to each Company Data Subject and the purpose for such collection / Processing.
2. Capitalised words and expressions used in this **Annexure C** but not otherwise defined shall have the meanings ascribed thereto in the Policy to which this **Annexure C** is attached or in POPI.
3. For purposes of this **Annexure C**, unless the context indicates otherwise, the following words and expressions shall bear the following meanings:
  - 3.1 **"FICA"** – the Financial Intelligence Centre Act No. 38 of 2001;
  - 3.2 **"FICA Documents"** means the following documentation in order to ensure compliance with FICA:
    - 3.2.1 a juristic person's certificate of registration / incorporation (certified copy not older than 3 months);
    - 3.2.2 a juristic person's certificate of name change (if applicable) (certified copy not older than 3 months);
    - 3.2.3 proof of the person's registered address (certified copy not older than 3 months);
    - 3.2.4 the person's VAT registration certificate (certified copy not older than 3 months);
    - 3.2.5 the person's income tax registration certificate (certified copy not older than 3 months);
    - 3.2.6 in the case of a juristic person, proof that the individual representing the juristic person is authorised to act on its behalf, usually in the form of a resolution or a letter of authorisation (certified copy not older than 3 months);
    - 3.2.7 a juristic person's letterhead;
    - 3.2.8 in the case of a juristic person, proof of the juristic person's trading name and principal place of business, usually acquired by way of a site visit or submission of a certified copy (not older than 3 months) of an IRP5, a SARS tax return, a recent (not older than 3 months) utility bill or municipal rates and taxes account or a Telkom account (not older than 3 months);
    - 3.2.9 in the case of a natural person, that person's full names, date of birth, identity or passport number, a certified copy (not older than 3 months) of the person's identity document or passport, residential address, proof of residential address (e.g. a utility bill, municipal rates and taxes account or Telkom account, in each instance not older than 3 months), postal address, contact telephone numbers (home, work, facsimile and mobile) and email address.

## POPI Policy continued

### Annexure C – Particulars relating to company data subjects (continued)

Company data subject	Categories of personal information collected / processed	Purpose for collection / processing of personal information
<b>Tenants</b>	<ul style="list-style-type: none"> <li>- Applicable FICA Documents</li> <li>- Contact details</li> </ul>	<ul style="list-style-type: none"> <li>- Compliance with FICA</li> <li>- Preparation of lease and other agreements</li> <li>- Issuing invoices</li> <li>- Collecting arrears</li> </ul>
<b>Suppliers</b>	<ul style="list-style-type: none"> <li>- Applicable FICA Documents</li> <li>- Contact Details</li> <li>- BEE rating</li> <li>- BEE certificate expiry date</li> <li>- Locations serviced</li> <li>- Nature of work</li> <li>- If applicable, professional body affiliations and membership numbers</li> <li>- If applicable, public liability insurance policy number</li> <li>- If applicable, professional indemnity insurance policy number</li> <li>- If applicable, COIDA / Workman's Compensation policy number</li> <li>- If applicable, details of other insurance policies and policy numbers</li> <li>- Trade references</li> <li>- Bank details</li> <li>- Latest financial statements</li> </ul>	<ul style="list-style-type: none"> <li>- Compliance with FICA</li> <li>- Requesting services</li> <li>- Settling invoices / accounts</li> <li>- Audit purposes (e.g. BEE verification audit)</li> </ul>
<b>Shareholders</b> via the Company's securities register manager, Computershare, which has a POPI policy aligned to the principles contained in the Company's POPI Policy and is available at <a href="https://www.computershare.com/za/Pages/privacy-policy.aspx">https://www.computershare.com/za/Pages/privacy-policy.aspx</a>	<ul style="list-style-type: none"> <li>- Full names</li> <li>- Business, residential or postal address</li> <li>- Email address</li> <li>- Registration or identity number</li> <li>- Number of securities held</li> <li>- Date on which securities were acquired / transferred and from / to whom they were acquired / transferred</li> <li>- Consideration paid for securities</li> </ul>	<ul style="list-style-type: none"> <li>- Maintain share register</li> <li>- Send notices / other communications</li> <li>- Settle distributions</li> </ul>
<b>Brokers</b>	<ul style="list-style-type: none"> <li>- Full names</li> <li>- Contact details</li> </ul>	<ul style="list-style-type: none"> <li>- Distributing vacancy schedules</li> <li>- Sending correspondence in relation to properties</li> </ul>
<b>Analysts</b>	<ul style="list-style-type: none"> <li>- Full names</li> <li>- Contact details</li> </ul>	<ul style="list-style-type: none"> <li>- Corresponding in relation to financial results and/or marketrelated information</li> <li>- Inviting to results presentations, roadshows and other events</li> </ul>
<b>Employees, directors, interns, learners and scholarship / bursary recipients</b>	<ul style="list-style-type: none"> <li>- Full names</li> <li>- Contact details</li> <li>- Curriculum vitae including contact details for references</li> <li>- If applicable, disclosure of directorships and/or interests</li> <li>- If applicable, references</li> <li>- If applicable, proof of registration with tertiary education institution</li> <li>- If applicable, academic transcripts</li> <li>- If applicable, details relating to financial standing / resources</li> <li>- ID number and demographic data (i.e. age, gender, race)</li> <li>- Banking and tax details</li> <li>- Income tax number</li> <li>- All details in terms of the company employee take-on form</li> <li>- Disclosures made by directors in terms of the Companies Act 71 of 2008</li> <li>- Emergency contact details</li> </ul>	<ul style="list-style-type: none"> <li>- Recruitment process including evaluating and interviewing candidates / applicants</li> <li>- Processing of payroll</li> <li>- Reporting to SARS</li> <li>- B-BBEE audit</li> <li>- Reporting under EEA, SDA</li> <li>- Administration to Medical Aid insurance</li> <li>- Administration of all company policies</li> <li>- Sustainability ratings</li> </ul>

## POPI Policy continued

### Annexure D – POPI notice and consent form

Please submit completed form to the company's information officer

We are committed to safeguarding and processing your personal information in a lawful manner. If, for any reason, you think that your personal information is not being processed in the correct manner, or that your personal information is being used for a purpose other than for what it was originally intended, please contact our information officer.

You may request access to the information we hold about you at any time. If you think we have outdated or incorrect information, please request us to update or correct it.

Please see **Annexure C** to our POPI policy (available on our website or on request from our information officer), which sets out which of your personal information is collected and the purpose(s) for which we process your personal information.

#### Consent to disclose and share your personal information

We may need to share your personal information in order to compile reports and/or analyses. When we share your personal information, we will take all precautions to ensure that the third party to whom the information is disclosed will treat your personal information with the same level of protection afforded by us. Your personal information may be hosted on servers managed by a thirdparty service provider.

##### A. Confirmation

I hereby confirm that I have familiarised myself with Equites Property Fund Limited's POPI Policy, particularly the applicable portions of **Annexure C** thereto.

##### B. Authorisation

I hereby consent to and authorise the Equites Property Fund Limited to share my Personal Information in accordance with its POPI Policy.

##### C. Signature

Signature

Date

## POPI Policy continued

### Annexure E – Sample consent and confidentiality clauses to be included in company employment agreement

#### 1. POPI consent and confidentiality

- 1.1 For purposes of this clause 1:
  - 1.1.1 “**Personal Information**” shall have the meaning ascribed to the term in POPI;
  - 1.1.2 “**POPI**” means the Protection of Personal Information Act No. 4 of 2013, as amended from time to time;
  - 1.1.3 “**POPI Policy**” means the Employer’s POPI policy.
- 1.2 The Employer undertakes to process the Personal Information of the Employee only in accordance with the conditions of lawful processing as set out in terms of POPI and in terms of the Employer’s POPI Policy and only to the extent that it is necessary to discharge its obligations and to perform its functions as an Employer and within the framework of the employment relationship and as required by South African law.
- 1.3 The Employee acknowledges that the collection of [his/her] Personal Information is necessary falls within the scope of execution of the legal functions and obligations of the Employer. The Employee accordingly irrevocably and unconditionally:
  - 1.3.1 confirms that [he/she] has been notified of the purpose and reason for the collection and processing of [his/her] Personal Information insofar as it relates to the discharge of the Employer’s obligations and the performance of its functions as an employer;
  - 1.3.2 consents and authorises the Employer to undertake the collection, processing and further processing of the Employee’s Personal Information for the purposes of securing and further facilitating the Employee’s employment with the Employer;
  - 1.3.3 without derogating from the generality of the foregoing, the Employee consents to the Employer’s collection and processing of Personal Information pursuant to any of the Employer’s internal policies in place insofar as Personal Information of the Employee is contained in relevant electronic communications;
  - 1.3.4 to make available to the Employer all necessary Personal Information required by the Employer for the purpose of securing and further facilitating the Employee’s employment with the Employer;
  - 1.3.5 to absolve the Employer from any liability in terms of POPI for failing to obtain the Employee’s consent or to notify the Employee of the reason for the processing of any of the Employee’s Personal Information;
  - 1.3.6 to the disclosure of [his/her] Personal Information by the Employer to any third party, where the Employer has a legal or contractual duty to disclose such Personal Information;
  - 1.3.7 the Employee further agrees to the disclosure of [his/her] Personal Information for any reason enabling the Employer to carry out or to comply with any business obligation the Employer may have or to pursue a legitimate interest of the Employer in order for the Employer to perform its business on a daytoday basis;
  - 1.3.8 the Employee authorises the Employer to transfer [his/her] Personal Information outside of the Republic of South Africa for any legitimate business purpose of the Employer within the international community.
- 1.4 The Employer undertakes not to transfer or disclose the Employee’s Personal Information unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.
- 1.5 The Employee acknowledges that during the course of the performance of [his/her] duties [he/she] may gain access to and become acquainted with the Personal Information of certain clients, suppliers and other Employees or Company Data Subjects (as defined in the POPI Policy). The employee will treat such Personal Information as a confidential business asset and agrees to respect the privacy of the person(s) to whom such information relates.
- 1.6 To the extent that the Employee is exposed to, or insofar as Personal Information of other employees or third parties are disclosed to the Employee, the Employee hereby agrees to be bound by appropriate and legally binding confidentiality and nonusage obligations in relation to such Personal Information.
- 1.7 The Employee acknowledges and agrees that [he/she] may not directly or indirectly utilise, disclose or make public in any manner to any person or third party, either within the Employer’s organisation or externally, any Personal Information unless such information is already publicly known or the disclosure is necessary in order for the Employee to perform [his/her] duties on behalf of the Employer.

## POPI Policy continued

### Annexure F – Sample service level agreement confidentiality clause

#### 1. Confidentiality

- 1.1 For purposes of this clause 1:
  - 1.1.1 “**Personal Information**” shall have the meaning ascribed to the term in POPI;
  - 1.1.2 “**POPI**” means the Protection of Personal Information Act No. 4 of 2013, as amended from time to time;
  - 1.1.3 “**POPI Policy**” means the Employer’s POPI policy.
- 1.2 The Parties acknowledge that pursuant to this Agreement the Parties may come into contact with, or have access to, Personal Information and other information that may be classified, or deemed as private or confidential and for which the other Party is responsible under POPI. Such Personal Information may also be deemed or considered as private and confidential as it relates to any third party directly or indirectly associated with this Agreement.
- 1.3 Each Party warrants to the other that it has the necessary consent to share or disclose the Personal Information.
- 1.4 Each Party agrees that it will at all times comply with POPI’s Regulations and Codes of Conduct and that it shall only collect, use and process Personal Information it comes into contact with pursuant to this Agreement in a lawful manner, and only to the extent required to execute the services, or to provide the goods and to perform its obligations under this Agreement.
- 1.5 Each Party agrees that it shall put in place, and at all times maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of Personal Information that it, or its employees, its contractors or other authorised individuals comes into contact with pursuant to this Agreement.
- 1.6 Unless so required by law, each Party agrees that it shall not disclose any Personal Information to any third party without the prior written consent of the other Party.

## POPI Policy continued

### Annexure G – Data processing agreement for operators

#### Data processing agreement

between

#### **Equites Property Fund Limited**

(Company Registration Number: 2013/080877/06)

("Company")

and

.....  
*Company name*

.....  
*(Entity Registration/Identity Number)*

("Service Provider")

## POPI Policy continued

### Annexure G – Data processing agreement for operators (continued)

#### 1. Definitions and interpretation

- 1.1 All terms defined in the Main Agreement shall, unless the context otherwise requires, bear the same meaning in this agreement.
- 1.2 In the agreement, unless the context otherwise requires:
- 1.2.1 **“Company’s Personal Information”** means personal information provided or made available to the Service Provider by (or collected or created for) the Company in connection with the Main Agreement.
- 1.2.2 **“Data Subject”** means the person to whom personal information relates;
- 1.2.3 **“Data Breach”** means any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, any of the Company’s Personal Information;
- 1.2.4 **“Data Protection Losses”** means all liabilities and amounts, including all: costs (including legal costs), claims, demands, actions, settlements, losses, liabilities and damages, administrative fines or penalties imposed by a regulatory authority, compensation to a Data Subject ordered by a regulatory authority, and the reasonable costs of compliance with investigations by a regulatory authority, and any loss or corruption of the Company’s Personal Information including the costs of rectification or restoration of the Company’s Personal Information;
- 1.2.5 **“Effective Date”** means the date this agreement is signed by the last party signing;
- 1.2.6 **“Main Agreement”** means the service or other agreement(s) entered into, or to be entered into between the Company and the Service Provider in terms of which the Service Provider provides services to the Company;
- 1.2.7 **“Operator”** shall have the meaning ascribed to the term in POPI;
- 1.2.8 **“Parties”** means the Company and the Service Provider;
- 1.2.9 **“Personal Information”** shall have the meaning ascribed to the term in POPI;
- 1.2.10 **“POPI”** means the Protection of Personal Information Act No. 4 of 2013, as amended from time to time;
- 1.2.11 **“POPI Policy”** means the Company’s POPI policy;
- 1.2.12 **“Processing”** shall have the meaning ascribed to the term in POPI.
- 1.2.13 **“Processing Instructions”** means the instructions for processing the Company’s Personal Information, as set out in this agreement, the Main Agreement, and otherwise as provided by or on behalf of the Company to the Service Provider;
- 1.2.14 **“Regulator”** means the Information Regulator established in terms of section 39 of POPI; and
- 1.2.15 **“Responsible Party”** shall have the meaning ascribed to the term in POPI.
- 1.3 In the event of conflict or inconsistency between the provisions of this agreement and the main terms of the Main Agreement, the provisions contained in this agreement shall prevail to the extent of the inconsistency, provided always that nothing in this agreement shall permit the Service Provider to process the Company’s Personal Information in a manner which is prohibited by the Main Agreement.

#### 2. Duration

- 2.1 This agreement shall commence on the Effective Date and shall endure for as long as the Main Agreement, or any other agreement between the Parties, are in effect.

## POPI Policy continued

### Annexure G – Data processing agreement for operators (continued)

#### 3. Processing

- 3.1 For purposes of this agreement, the Company is the Responsible Party in respect of the Company's Personal Information.
- 3.2 The Company's Personal Information shall be provided by or on behalf of the Company to the Service Provider for the purpose of enabling the Service Provider to provide the services or access to the Company's Personal Information shall be granted to the Service Provider during the provision of the services.
- 3.3 For purposes of this agreement, the Service Provider is an Operator, acting on the Company's behalf. Processing of the Company's Personal Information shall be undertaken by the Service Provider in accordance with this agreement.
- 3.4 As Operator, the Service Provider will only act upon and process the Company's Personal Information in accordance with the Processing Instructions. The Company's Personal Information will be used by the Service Provider in accordance with and for the purposes set out in the Processing Instructions and only where necessary to provide the services to the Company.
- 3.5 If the Service Provider is ever unsure as to the parameters or lawfulness of the instructions issued by the Company, the Service Provider shall, as soon as reasonably practicable, revert to the Company for the purpose of seeking clarification or further instructions.
- 3.6 The Service Provider shall:
- 3.6.1 comply with and process the Company's Personal Information in accordance with POPI; and
- 3.6.2 immediately notify the Company, if in its opinion, an instruction infringes POPI.
- 3.7 The Service Provider shall cooperate and promptly (and in any event within forty-eight hours) assist the Company with any information request received from the Regulator or Data Subjects, pertaining to the Company's Personal Information and the services.
- 3.8 The Service Provider shall maintain a record of all categories of processing activities carried out on behalf of the Company containing as a minimum the information required under POPI, which shall be made available to the Company upon request.

#### 4. The service provider's employees

- 4.1 The Service Provider shall ensure that its employees will not process the Company's Personal Information:
- 4.1.1 except in accordance with the provisions of this agreement; and
- 4.1.2 procure that its employees are contractually obligated to maintain the security and confidentiality of the Company's Personal Information and this obligation continues even after their engagement ends.
- 4.2 The Service Provider shall take all reasonable steps to ensure the reliability of the employees processing the Company's Personal Information and that such employees receive adequate training on compliance with this agreement and POPI.

#### 5. Rights management

- 5.1 Should the Company request or require the Service Provider to use the Company's Personal Information for a new or supplementary purpose (a purpose outside the scope of the Main Agreement), then the Service Provider must obtain appropriate consent from the Data Subjects concerned.
- 5.2 In so doing, the Service Provider must obtain consent from a parent or guardian, before collecting the personal information of or relating to a child.
- 5.3 If the Service Provider discovers that it has collected a child's personal information, without consent from a parent or legal guardian where such consent should have been obtained, the Service shall immediately delete such information.

## POPI Policy continued

### Annexure G – Data processing agreement for operators (continued)

#### 6. Storage of the company's personal information

- 6.1 The Service Provider shall adhere to the Company's storage policies and instructions (as amended from time to time), including but not limited to:
- 6.1.1 the Company's Personal Information must only be hosted and stored on solutions approved by the Company;
  - 6.1.2 the Company's Personal Information must not be stored on publicly available cloud storage solutions; and
  - 6.1.3 the Company's Personal Information must not be stored on portable devices.

#### 7. Retention, deletion or return of the company's personal information

- 7.1 The Service Provider shall, at the Company's request and in accordance with the Company's instructions, securely retain, delete or return all copies of the Company's Personal Information by secure file transfer in such format as the Company reasonably requests and cease processing the Company's Personal Information after the business purposes for which the Company's Personal Information was collected or transferred have been fulfilled, or earlier upon the Company's written request.

#### 8. Disclosure

- 8.1 The Service Provider shall implement appropriate technical and organisational measures to ensure that the Company's Personal Information is only disclosed to the Service Provider's employees and authorised sub-Operators who need to know such information to be able to provide the services.
- 8.2 The Service Provider shall promptly inform the Company (and in any event within 48 hours) should it receive any request for disclosure of the Company's Personal Information or a complaint in relation to either of the Parties obligations under POPI and shall provide the Company with full details of such request or complaint.

#### 9. Security measures

- 9.1 The Service Provider agrees that it has implemented and will maintain throughout the duration of this agreement appropriate technical and organisational measures, internal controls and information security routines intended to protect the Company's Personal Information against accidental, unauthorised, or unlawful access, disclosure, alteration, loss, or destruction, which shall at all times be:
- 9.1.1 of at least the minimum standard required by POPI; and
  - 9.1.2 so as to ensure a level of security for the Company's Personal Information appropriate to the risk.

#### 10. Data breaches

- 10.1 Should the Service Provider become aware of or has reasonable grounds to believe that any Data Breach has occurred, the Service Provider shall immediately (and in any event within 24 hours):
- 10.1.1 notify the Company in writing of the Data Breach and provide sufficient information to enable the Company to report the Data Breach to the Regulator and/or notify affected Data Subjects, as required under POPI;
  - 10.1.2 investigate the Data Breach and provide the Company with detailed information about the Data Breach;
  - 10.1.3 take reasonable steps to mitigate the effects and to minimise any damage resulting from the Data Breach and assist the Company in remediating or mitigating any potential damages from a Data Breach to the extent that such remediation or mitigation is within the Service Provider's control as well as reasonable steps to prevent a recurrence of such Data Breach; and
  - 10.1.4 at the Company's request cooperate in adequately informing the Regulator and/or affected Data Subjects as so directed by the Company.

## POPI Policy continued

### Annexure G – Data processing agreement for operators (continued)

#### 11. Sub-operators

- 11.1 The Service Provider shall not permit sub-Operators to process the Company's Personal Information, without the prior written consent of the Company.
- 11.2 The Service Provider shall ensure sub-Operators are contractually bound to the same obligations as are contained in this agreement. The Service Provider shall also remain fully liable to the Company for a sub-Operator's performance of the contract, as well as for any acts or omissions of the sub-Operator in regard to its processing of the Company's Personal Information.

#### 12. International transfer of data

- 12.1 The Service Provider shall only transfer the Company's Personal Information from the Republic of South Africa to another country or an international organisation, where such transfer:
- 12.1.1 has been approved in writing by the Company; and
- 12.1.2 otherwise complies with POPI.

#### 13. Audits

- 13.1 Subject to reasonable notice, the Service Provider shall permit the Company and/or a qualified representative of the Company to conduct during normal working hours periodic security scans and audits of Service Provider's systems and processes in relation to the Processing of the Company Personal Information and shall comply with all reasonable requests or directions by the Company to verify and/or procure that the Service Provider is in full compliance with its obligations under this agreement and Data Protection Legislation.
- 13.2 The Service Provider shall promptly resolve, at its own expense, all security issues and other non-compliance discovered by the Company and reported to the Service Provider.

#### 14. Warranties

- 14.1 The Company represents and warrants that it shall comply with POPI requirements at all times.
- 14.2 The Service Provider represents and warrants that:
- 14.2.1 it shall comply with POPI requirements at all times; and
- 14.2.2 the processing of the Company's Personal Information by the Service Provider in accordance with the Processing Instructions from time to time shall not cause the Company to be in breach of POPI requirements.
- 14.3 The Service Provider shall indemnify the Company on demand and shall at all times keep the Company indemnified in respect of all Data Protection Losses suffered or incurred by the Company or its subsidiaries, arising directly or indirectly from or in connection with:
- 14.3.1 any breach by the Service Provider of its obligations under POPI or its obligations under this agreement; or
- 14.3.2 the Service Provider (or any person acting on its behalf) acting outside or contrary to the lawful Processing Instructions of the Company in respect of the processing of the Company's Personal Information.
- 14.4 Any financial caps or limitation of liability set out in the Main Agreement shall not apply to this indemnity.

#### 15. Breach

- 15.1 Should the Service Provider commit a breach of any term of this agreement or the Processing Instructions, such breach shall be regarded a material breach.
- 15.2 Should the Service Provider commit a breach of any term of this agreement or the Processing Instructions, then the Company shall be entitled to give the Service Provider 7 (seven) working days' notice in writing to remedy such breach, and if the Service Provider fails to comply with such notice, then the Company shall immediately be entitled, but not obliged, notwithstanding the provisions of the Main Agreement and without prejudice to any other rights or remedies which it may have in law, including the right to claim damages:
- 15.2.1 to cancel the Main Agreement and/or relevant work orders, or
- 15.2.2 to claim specific performance.

## POPI Policy continued

### Annexure G – Data processing agreement for operators (continued)

SIGNED at \_\_\_\_\_ on \_\_\_\_\_ 2021.

.....  
*Name of service provider*

SIGNED at \_\_\_\_\_ on \_\_\_\_\_ 2021.

For and on behalf of  
**Equites Property Fund Limited**

.....  
*Signature*

.....  
*Name of signatory*

.....  
*Designation of signatory*

## POPI Policy continued

### Annexure G – Data processing agreement for operators (continued)

SIGNED at \_\_\_\_\_ on \_\_\_\_\_ 2021.

For and on behalf of  
**Equites Property Fund Limited**

.....  
*Signature*

.....  
*Name of signatory*

.....  
*Designation of signatory*



**Cape Town  
(Head Office)**

+27 21 460 0404  
14th Floor, Portside Tower  
4 Bree Street  
Cape Town  
8001  
South Africa

**Johannesburg**

+27 10 286 0469  
4 Meadowview Lane  
Equites Park, Meadowview  
Linbro Park  
2065  
South Africa