

# 8TH SEASON CAPITAL (PTY) LTD

## PROTECTION OF PERSONAL INFORMATION & DATA PROTECTION POLICY

OCTOBER 2023

**Date of issue/update**

Created: 01 October 2023

Last reviewed and/or updated: 30 November2023

Version 1

**Policy owner / Thabo Ncalo**

**Approved by**

Chief Executive Officer / Key Individual

## **1. Personal Information:**

Personal information is collected only when an individual knowingly and voluntarily submits information. Personal Information may be required to provide an individual with further services or to answer any requests or enquiries relating to this service.

It is 8<sup>th</sup> Season Capital (herein referred to as the “Financial Services Provider (FSP)”) intention that this policy will protect an individual’s personal information from being prejudiced in any way and this policy is consistent with the privacy laws applicable in South Africa.

As an FSP, we collect, store and use the personal information provided by a natural / juristic person, to provide financial services.

## **2. Use of Information:**

Our FSP needs to collect personal or other information – which might include the following:

- KYC and other required client verification
- For underwriting purposes;
- Conducting credit reference searches or verification;
- Confirming and verifying an individual’s identity;
- For credit assessment and credit management;
- For the detection and prevention of fraud, crime, money laundering or other malpractice;
- Conducting market or customer satisfaction research;
- For audit and record keeping purposes;
- In connection with legal proceedings;
- Follow an individual’s instructions;
- Inform an individual of services;
- Make sure the FSPs business suits the individual’s needs.

Personal information that an individual submits is used only for the purpose for which it was intended. Copies of correspondence that may contain personal information, is stored in archives for record-keeping and back-up purposes only.

The FSP will not, without an individual’s consent, share information with any other third parties, other than where required by law for any purposes whatsoever.

## **3. Security**

The FSP strives to ensure the security, integrity and privacy of personal information submitted. The FSP will review and update its security measures in accordance with future legislation and technological advances. Unfortunately, no data transmission over the Internet can be guaranteed to be totally secure, however, the FSP will endeavour to take all reasonable steps to protect the personal information, which an individual submits to the FSP or to the FSPs online products and services. The FSP will always set the highest standards to ensure the integrity of their systems.

The FSP may engage with other organisations to provide support services to the FSP. Third Parties are obliged to respect the confidentiality of any personal information held by the FSP. A Service Level agreement is in place with all Third parties to ensure adherence to all Privacy Policies.

The FSPs employees are obliged to respect the confidentiality of any personal information held by the FSP. All employees are required to sign an employment contract which includes a confidentiality clause.

The FSP will not reveal any personal information to anyone unless:

- It is compelled to comply with legal and regulatory requirements or when it is otherwise allowed by law;
- It is in the public interest;
- The FSP needs to do so to protect their rights.

The FSP endeavours to take all reasonable steps to keep secure any information which they hold about an individual, and to keep this information accurate and up to date. If at any time, an individual discovers that information gathered about them is incorrect, they may contact the FSP to have the information corrected.

The FSP recognises the importance of protecting the privacy of information collected about individuals, information that is capable of identifying an individual (personal information).

#### **4. Contact information:**

Any questions relating to the FSPs privacy policy or the treatment of an individual's personal data may be addressed to the contact details below:

Information officer: Thabo Milton Ncalo

Telephone number: 083 690 3917

Address: 107 Katherine Street, Sandown, Sandton 2196

Email address: [thabo@8thseason.com](mailto:thabo@8thseason.com)

Website: [www.8thseason.com](http://www.8thseason.com)

# 8th Season Capital - Data Protection Policy

## 1. INTRODUCTION AND PURPOSE

- 1.1. This policy ("Policy") sets out the data protection principles and procedures of 8th Season Capital(Pty) Ltd, an investment management and property development entity (Registration No. 2016/185527/07), whose registered office is at 107 Katherine Street, Sandown, Sandton 2196 (the "Organisation").
- 1.2. In particular, this Policy summarises how the Organisation processes personal information belonging to, amongst others, applicants for funding, portfolio companies, business contacts, partners, and contractors ("data subjects").
- 1.3. The Organisation takes the privacy of personal information very seriously, and is committed to processing personal information in accordance with data protection legislation, including the Protection of Personal Information Act (No. 4 of 2013) ("POPI Act") and, where applicable, the General Data Protection Regulation (EU 2016/679) ("GDPR"), which includes the retained EU law version of GDPR as it forms part of the law of the United Kingdom, and any other data protection legislation and/or regulation applicable to the Organisation (collectively, the "Data Protection Laws").
- 1.4. This Policy is made available on the Organisation's website (<https://www.8thseason.com/>) and is otherwise available in hard copy, on request.
- 1.5. The Organisation's Information Officers' details are as set out below:
  - Telephone number: 083 690 3917
  - Address: 107 Katherine Street, Sandown, Sandton, 2196
  - Email address: [thabo@8thseason.com](mailto:thabo@8thseason.com)
  - Website: [www.8thseason.com](http://www.8thseason.com)
- 1.5. This Policy uses terminology defined in POPI (these terms appear in bold). Please see paragraph 23 of this Policy where this terminology is defined and for guidance in interpreting this Policy.

## 2. SCOPE

The procedures and principles set out in this Policy must be followed at all times by the Organisation's angels, employees, agents, contractors, affiliates, and other parties working on behalf of the Organisation, including third-party operators processing personal information on the Organisation's behalf. No personal information must be processed for or on the Organisation's behalf unless processed in accordance with this Policy.



### 3. INFORMATION OFFICERS

- 3.1 The Information Officers are responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.
- 3.2 The Information Officers are tasked with ensuring that all angels, employees, agents, contractors, affiliates, and other parties working on behalf of the Organisation, including third-party operators, comply with this Policy and, where applicable, implement all such practices, processes, controls, and training as is reasonably necessary to ensure such compliance.
- 3.3 Any questions relating to this Policy or to Data Protection Laws should be referred to the Organisation's Information Officers.
- 3.4 The Organisation's employees, agents, contractors, affiliates, and other parties working on behalf of the Organisation, including third-party operators processing personal information on the Organisation's behalf must consult the Information Officers in the following cases:
  - 3.4.1. if there is any uncertainty relating to the lawful basis on which personal information is to be collected, held, and/or processed;
  - 3.4.2. if consent is being relied upon in order to collect, hold, and/or process personal information;
  - 3.4.3. if there is any uncertainty relating to the retention period for any particular type(s) of personal information;
  - 3.4.4. if any new or amended privacy notices or similar privacy-related documentation are required;
  - 3.4.5. if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of a subject's request/s);
  - 3.4.6. if a personal information breach (whether suspected or actual) has occurred;
  - 3.4.7. if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal information;
  - 3.4.8. if personal information is to be shared with third parties (whether such third parties are acting jointly as responsible parties or operators);
  - 3.4.9. if personal information is to be transferred outside of the country in which it is originally processed and there are questions relating to the legal basis on which to do so;
  - 3.4.10. when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities;
  - 3.4.11. when personal information is to be used for purposes different to those for which it was originally collected;
  - 3.4.12. if any automated processing, including profiling or automated decision-making, is to be carried out; or
  - 3.4.13. if any assistance is required in complying with the law applicable to direct marketing.

#### **4. THE RIGHTS OF DATA SUBJECTS**

Data subjects have the right to have their personal information processed in accordance with the conditions for the lawful processing of personal information as referred to in [Chapter 3](#) of POPI. The Organisation is committed to upholding the rights of data subjects, which rights include:

- 4.1. the right to be notified;
- 4.2. the right of access;
- 4.3. the right to rectification;
- 4.4. the right to correction, destruction or erasure;
- 4.5. the right to object to or restrict processing;
- 4.6. the right to data portability;
- 4.7. rights with respect to automated decision-making and profiling;
- 4.8. the right to complain to the Regulator; and
- 4.9. the right to institute civil proceedings in relation to its personal information.

#### **5. DATA PROTECTION PRINCIPLES**

5.1. The Organisation is committed to promoting and upholding the conditions for the lawful processing of personal information as set out in POPI, being:

- 5.1.1. accountability, as contemplated in section 8;
- 5.1.2. processing limitation, as contemplated in sections 9 – 12;
- 5.1.3. purpose specification, as contemplated in sections 13 – 14;
- 5.1.4. further processing limitation, as contemplated in section 15;
- 5.1.5. information quality, as contemplated in section 16;
- 5.1.6. openness, as contemplated in sections 17 – 18;
- 5.1.7. security safeguards, as contemplated in sections 19 – 22; and
- 5.1.8. data subject participation, as contemplated in sections 23 – 25.

5.2. Accordingly, the Organisation is committed to processing personal information only in a manner that:

- 5.2.1. is lawful and transparent;
- 5.2.2. is specified, explicit, and legitimate, and for a particular purpose;
- 5.2.3. is relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- 5.2.4. is accurate;
- 5.2.5. permits identification of data subjects for no longer than is necessary or insofar as permitted by Data Protection Law; and
- 5.2.6. ensures appropriate security of the personal information, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures.



## **6. PROCESSING OF PERSONAL INFORMATION**

- 6.1. The Organisation shall only process personal information if at least one of the following apply:
- 6.1.1. the data subject (or a competent person, where the data subject is a child) consents to the processing;
  - 6.1.2. processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;
  - 6.1.3. processing complies with an obligation imposed by law on the responsible party;
  - 6.1.4. processing protects a legitimate interest of the data subject;
  - 6.1.5. processing is necessary for the proper performance of a public law duty by a public body; and/or
  - 6.1.6. processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.
- 6.2. Where a person transmits any personal information to the Organisation which belongs to a third party, that person must warrant that they are authorised to do so and that the processing of the personal information by the Organisation is lawful.

## **7. PROCESSING OF SPECIAL PERSONAL INFORMATION**

The Organisation shall only process special personal information in accordance with the provisions of Part B of POPI. The processing of special personal information shall be lawful if at least one of the following applies:

- 7.1. processing is carried out with the consent of a data subject;
- 7.2. processing is necessary for the establishment, exercise or defence of a right or obligation in law;
- 7.3. processing is necessary to comply with an obligation of international public law;
- 7.4. processing is for historical, statistical or research purposes to the extent that:
  - 7.4.1. the purpose serves a public interest and the processing is necessary for the purpose concerned; or
  - 7.4.2. it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;
- 7.5. information has deliberately been made public by the data subject; or
- 7.6. where applicable, the provisions of sections 28 to 33 of POPI, as the case may be, are complied with.

## **8. PROCESSING OF PERSONAL INFORMATION RELATING TO CHILDREN**

The Organisation shall only process personal information relating to a child in accordance with the provisions of Part C of POPI. The processing of personal information relating to a child shall be lawful if at least one of the following applies:

- 8.1. the processing is carried out with the prior consent of a competent person;
- 8.2. the processing is necessary for the establishment, exercise or defence of a right or obligation in law;



- 8.3. the processing is for historical, statistical or research purposes to the extent that:
  - 8.3.1. the purpose serves a public interest and the processing is necessary for the purpose concerned; or
  - 8.3.2. it appears to be impossible or would involve a disproportionate effort to ask for consent, and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the child to a disproportionate extent; and/or
- 8.4. the relevant personal information has deliberately been made public by the child with the consent of a competent person.

## 9. ACCURACY OF PERSONAL INFORMATION

- 9.1 The Organisation shall ensure that all personal information collected, processed, and held by it is kept accurate and up to date.
- 9.2. If any personal information is found to be inaccurate or out-of-date, the Information Officer must be notified immediately.

## 10. STORAGE AND RETENTION

- 10.1. Personal data, is stored by the Organisation in the following ways and in the following locations:
  - 10.1.1. the Organisation's Google Drive account, hosted on Google's various remote servers, which account is accessible by the Organisation's officers and investor partners;
  - 10.1.2. the Organisation's DropBox account, hosted using various remote servers, which account is accessible by the Organisation's officers and investor partners; and
  - 10.1.3. computers and mobile devices owned by the Organisation's employees, agents, and contractors.
- 10.2. When personal information is no longer required, it will either be de-identified, or all reasonable steps will be taken to erase or otherwise dispose of it without delay.

## 11. SECURE PROCESSING

- 11.1. The Organisation shall ensure that all personal information collected, held, and processed by it is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage.
- 11.2. All technical and organisational measures taken to protect personal information shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal information.
- 11.3. The Organisation will adhere to the following guidelines to protect against the confidentiality, integrity, and availability of all personal information:
  - 11.3.1. only those with a genuine need to access and use personal information and who are authorised to do so may access and use it;
  - 11.3.2. personal information must be accurate and suitable for the purpose for which it is collected, held, and processed; and
  - 11.3.3. authorised users must always be able to access the personal information as required for the authorised purpose or purposes.





## **12. ACCOUNTABILITY AND RECORD-KEEPING**

- 12.1. A data protection impact assessment shall be conducted if any processing of personal information presents a significant risk to the rights and freedoms of data subjects.
- 12.2. The Organisation's data protection compliance shall be regularly reviewed and evaluated by the Information Officer.
- 12.3. The Organisation will keep adequate internal records in respect of the processing of personal information.

## **13. DATA SUBJECT ACCESS**

- 13.1. Data subjects may, at any time, request an Information Officer to supply details as to the personal information which the Organisation holds about that data subject, what the Organisation is doing with that personal information, and why.
- 13.2. The Organisation does not charge a fee for the handling of normal requests. However, the Organisation reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

## **14. RECTIFICATION OF PERSONAL INFORMATION**

- 14.1. Data subjects have the right to require the Organisation to rectify any of their personal information that is inaccurate or incomplete. The Organisation shall comply with such requests timeously.
- 14.2. In the event that any affected personal information has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal information.

## **15. ERASURE OF PERSONAL INFORMATION**

- 15.1. Data subjects have the right to request that the Organisation erases the personal information it holds about them in certain circumstances, for example, where the data subject withdraws its consent for the processing of its personal information.
- 15.2. Unless the Organisation has reasonable grounds to refuse to erase personal information, all requests for erasure shall be complied with timeously, and the data subject informed of the erasure.
- 15.3. If any personal information that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

## **16. RESTRICTION OF PERSONAL INFORMATION PROCESSING**

- 16.1. A data subject may request that the Organisation ceases processing the personal information it holds about them. If a data subject makes such a request, the Organisation shall retain only the amount of personal information concerning that data subject (if any) that is necessary to ensure that the personal information in question is not processed further, or unless otherwise required by law.



- 16.2. If any affected personal information has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## **17. DATA PORTABILITY**

Data subjects have the right to receive a copy of their personal information in the Organisation's possession in a structured, commonly used and machine-readable format, and to request its transmission to another entity.

## **18. OBJECTIONS TO PROCESSING PERSONAL INFORMATION**

- 18.1. Data subjects have the right to object to the Organisation processing their personal information based on legitimate interests, for direct marketing (including profiling), and processing for research and statistics purposes.
- 18.2. Where a data subject objects to the Organisation processing their personal information based on its legitimate interests, the Organisation shall cease such processing immediately, unless it can be demonstrated that the Organisation's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.
- 18.3. Where a data subject objects to the Organisation processing their personal information for direct marketing purposes, the Organisation shall cease such processing promptly.
- 18.4. Where a data subject objects to the Organisation processing their personal information for research and statistics purposes, the data subject must demonstrate grounds relating to his or her particular situation. The Organisation is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.

## **19. DIRECT MARKETING**

- 19.1. The Organisation shall obtain a data subject's prior consent for direct marketing (including email and text messaging) and shall not approach a data subject more than once for the purpose of obtaining their consent to direct marketing.
- 19.2. If a data subject objects to direct marketing, the Organisation shall comply with the request promptly.
- 19.3. The Organisation will not approach a data subject for purposes of direct marketing if that data subject has previously withheld consent.

## **20. TECHNICAL AND ORGANISATIONAL SECURITY MEASURES**

- 20.1. Where possible, the following technical and organisational measures shall be implemented to protect the security of personal information:
- 20.1.1. all personal information transferred physically should be transferred in a suitable container and marked "confidential";
- 20.1.2. all hardcopies of personal information, along with any electronic copies stored on physical media shall be stored securely and appropriate access control measures shall be implemented;



- 20.1.3. no personal information shall be shared informally, and if access is required in respect of any personal information, such access should be requested in writing;
- 20.1.4. personal information shall be handled with care at all times and should not be left unattended;
- 20.1.5. all electronic copies of personal information shall be stored securely using passwords and where appropriate, encrypted.

## **21. TRANSFERRING PERSONAL DATA ACROSS BORDERS**

The Organisation may, from time to time, transfer personal information to countries outside of the country in which the personal information was collected, but only where one of the following principles applies:

- 21.1. the third party who is the recipient of the information is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection that:
  - 21.1.1. effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and,
  - 21.1.2. includes provisions, that are substantially similar to this section, relating to the further transfer of personal information from the recipient to third parties who are in a foreign country;
- 21.2. the data subject consents to the transfer;
- 21.3. the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures taken in response to the data subject's request;
- 21.4. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the responsible party and a third party; or
- 21.5. the transfer is for the benefit of the data subject, and:
  - 21.5.1. it is not reasonably practicable to obtain the consent of the data subject to that transfer;
  - 21.5.2. if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

## **22. PERSONAL INFORMATION BREACH NOTIFICATION**

- 22.1. All personal information breaches must be reported immediately to the Organisation's Information Officer.
- 22.2. If an angel, employee, agent, contractor, or other party working on behalf of the Organisation becomes aware of or suspects that a personal information breach has occurred, they shall notify an Information Officer immediately, and shall not attempt to investigate it themselves. All evidence relating to the personal information breach in question should be carefully retained.
- 22.3. Where there are reasonable grounds to believe that the personal information of a data subject has been accessed or acquired by any unauthorised person, the Organisation shall, as soon as reasonably possible, notify, in writing:



- 22.3.1. the Regulator (such notification to be within 72 hours, where GDPR is applicable); and
- 22.3.2. the data subject, unless the identity of such data subject cannot be established.
  
- 22.4. The notification referred to in clause 25.3 shall include, at a minimum, the following information:
  - 22.4.1. a description of the possible consequences of the security compromise;
  - 22.4.2. a description of the measures that the responsible party intends to take or has taken to address the security compromise;
  - 22.4.3. a recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise; and
  - 22.4.4. if known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.
  
- 22.5. The Organisation may only delay notification of the data subject if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

## 23. DEFINITIONS

1. In this Policy, the following words mean:

- 23.1.1. **child.** A natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning him- or herself.
- 23.1.2. **competent person.** Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
- 23.1.3. **consent.** Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
- 23.1.4. **de-identify.** In relation to personal information of a data subject, to delete any information that:
  - 23.1.4.1. identifies the data subject;
  - 23.1.4.2. can be used or manipulated by a reasonably foreseeable method to identify the data subject; or
  - 23.1.4.3. can be linked by a reasonably foreseeable method to other information that identifies the data subject, and “de-identified” has a corresponding meaning.
- 23.1.5. **Information Officer.** As contemplated in POPI Act.
- 23.1.6. **operator.** A person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
- 23.1.7. **personal information.** Any information relating to a data subject who can be identified, directly or indirectly, by reference to an identifier such as a name, identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that data subject.



- 23.1.8. **personal information breach.** A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal information transmitted, stored, or otherwise processed.
- 23.1.9. **process.** Any operation or set of operations performed on personal information or sets of personal information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- 23.1.10. **Regulator.** The Information Regulator established in terms of section 39 of POPI Act.
- 23.1.11. **responsible party.** A public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
- 23.1.12. **special personal information.** As contemplated in section 26 of POPI Act, which includes religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; and/or the criminal behaviour of a data subject to the extent that such information relates to:
- 23.1.12.1. the alleged commission by a data subject of any offence; or
- 23.1.12.2. any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

## 23.2 In this Policy:

1. the words “include”, “including” and “in particular” are by way of example only and shall not limit the generality of any preceding words;
  2. if any provision becomes illegal, invalid or unenforceable, such provision shall be severed, to the extent of its illegality, invalidity or unenforceability, from the balance of this agreement; and
  3. the words “other” and “otherwise” shall be interpreted as widely as possible and will not be limited by any preceding words.
- 23.2. This Policy has been drafted using the terminology contemplated in POPI Act. Where this Policy is interpreted in the context of GDPR, the terms:
1. "Information Officer" shall be read as "Data Protection Officer";
  2. "responsible party " shall be read as " data controller";
  3. "personal information " shall be read as " personal data";
  4. "Regulator" shall be read as "Supervisory Authority"; and
  5. "special personal information" shall be read as "special category personal information", as those terms are defined in GDPR.