

PROTECTION OF PERSONAL INFORMATION POLICY

INTRODUCTION

Protection of Personal Information Act (POPI) gives effect to the constitutional right to privacy regulates the manner in which personal information may be processed, and provides rights and remedies to protect personal information.

POPI applies to the processing of PI by a responsible person domiciled in the Republic and where processing happens in the Republic. POPI will override other legislation that contains inconsistent provisions relating to the processing of PI, and where other legislation provides for more extensive conditions for the processing of PI the other legislation will prevail

PI relates to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including, but not limited to:

- race, gender, sex, pregnancy, marital status, national or ethnic origin, colour, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person;

Processing is any operation or activity, whether or not by automatic means, including:

- collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any form;
- merging, linking, as well a restriction, degradation, erasure or destruction.

Key concepts include:

- 'consent' – any voluntary, specific and informed expression agreeing to the processing of PI;
- 'Data Subject' – means the person to whom the PI relates;
- 'de-identify' – means to delete any information that:
 - identifies the data subject;

- can be used or manipulated to identify the data subject;
- can be linked to other information to identify the data subject;
- ‘Responsible Person’ – means any person that collects, receives, records, organises, collates, stores, updates, modifies, retrieves, alters, consults, uses, disseminates, distributes, merges, links, erase or destructs PI of the Data Subject. This list is not exhaustive.
- ‘Electronic communication’ – means the emission, transmission or reception of information, including without limitation, voice, sound, data, text, video, animation, visual images, moving images and pictures, signals or a combination thereof by means of magnetism, radio or other electromagnetic waves, optical, electro-magnetic systems or any agency of a like nature, whether with or without the aid of tangible conduct, but does not include content service.

“Genesis Capital Operations Committee “

Means a committee, consisting of one or more persons, appointed by the FSP, that is responsible to review a complaint, by a complainant that is dissatisfied with the outcome of the Officer.

1 Officer and Responsibility / Accountability

- 1.1 Genesis Capital hereby appoints Roland Salomon as the group Personal Protection of Personal Information Officer (Officer).
- 1.2 All persons, who collect, process, or use Personal Information (PI) shall be accountable to the Officer for such information.
- 1.3 This policy shall be made available via Genesis Capital website (www.gencapital.co.za), or a paper copy provided upon written request.
- 1.4 This Policy applies to any personal information supplied to a third party for processing.
- 1.5 The collection, use and retention of PI is done only, with the Officer’s written consent.
- 1.6 Any person suspecting that the information is being used for purposes other than that explicitly approved and collected for, may register a complaint with the Officer.
- 1.7 The Officer shall investigate the above complaint and inform the complainant of his findings and corrective action taken, if any.

- 1.8 If the complainant is dissatisfied with the findings of the Officer, an appeal may be submitted to the Genesis Capital Operations Committee. The determination made by the Genesis Capital Operations Committee will be final.
- 1.9 The Officer shall be responsible to give training to all Genesis Capital Staff and volunteers who might, collect, use or retain PI.

2 Purposes

PI must be collected for a specific, explicitly defined and lawful purpose related to the function or activity of the responsible party. The data subject must be made aware of the purpose of the collection.

Records must not be retained any longer than is necessary for achieving the purpose for which it was collected unless;

- further retention is required by law;
- the responsible party reasonably requires to keep it;
- retention is required by a contract between the parties;
- the data subject consents to the further retention.

PI must be destroyed, deleted or de-identified as soon as is reasonably practical. Destruction or deletion must be done in a manner that prevents its reconstruction in an intelligible form.

- 2.1 The Officer shall ensure that the information collected will not be used for any other purpose before obtaining the individual's approval, unless the new purpose is required by law.
- 2.2 The Officer shall ensure that a person collecting personal information will be able to explain to the individual why this is being done.
- 2.3 The Officer shall ensure that limited collection, limited use, disclosure, and retention principles are respected in identifying why personal information is to be collected.

3 Consent

- 3.1 When collecting PI, the responsible party shall obtain consent from the Data Subject, to use, collect, retain or disclose said PI.
- 3.2 When collecting PI, the responsible party shall ensure that the Data Subject understand, how the PI will be used.

- 3.3 Express consent will be obtained from the Data Subject, unless in the Officer's opinion implied consent will be acceptable. The consent must be clear and verifiable.
- 3.4 The reasonable expectations of the Data Subjects will be respected. (For example, the Data Subject may reasonably expect that by giving PI to the Responsible Party to sell a financial product, said PI will not be used to conduct market research. Nor will the Data Subject, reasonably expect that the PI will be given to a Third Party to contact the Data Subject)
- 3.5 The Data Subject may at any time withdraw consent given, subject to legal and contractual restrictions by giving reasonable notice.

4 Limiting Collection and Further Processing

- 4.1 The Responsible Party shall ensure that personal information will not be collected indiscriminately, but by fair and lawful means, and be limited to what is necessary to fulfil the specific purpose for which the PI is being collected.
- 4.2 PI may only be processed if:
 - the data subject consents to the processing;
 - processing is necessary for the conclusion or performance of a contract to which the data subject is a party;
 - there is a legal obligation to do the processing;
 - processing protects the legitimate interests of the data subject;
 - processing is necessary for the proper performance of a public law duty by a public body;
 - processing is necessary for the pursuit of legitimate interests of the responsible party.

A data subject may object, at any time, on reasonable grounds, to the processing of their PI. The responsible party may then no longer process the PI.

- PI must be collected directly from the data subject except if:
 - the information is contained in a public record or has deliberately been made public by the data subject;
 - the data subject has consented to the collection from another source;
 - collection from another source would not prejudice a legitimate interest of the data subject;
 - collection from another source is necessary:
 - to maintain law and order;
 - to enforce legislation concerning the collection of revenue;
 - for the conduct of court or tribunal proceedings;
 - in the interests of national security;
 - to maintain the legitimate interests of the responsible party.
 - compliance would prejudice a lawful purpose of the collection; or
 - compliance is not reasonably practicable in the circumstances of the particular case.
- 4.3 Further processing must be compatible with the purpose for which it was collected, unless the data subject gives consent to the further processing.

5 Direct Marketing

- 5.1 Direct marketing means unsolicited electronic communication. The processing of PI for the purpose of direct marketing by any form of electronic communication is prohibited unless the data subject:
- has given consent; or
 - is a customer of the responsible party and if:

- the responsible party has obtained the contact details of the data subject in the context of the sale of a product or service;
- it is for marketing the responsible parties own similar products or services; and
- if the data subject has been given reasonable opportunity to object, free of charge, at the time the information was collected or on the occasion of each communication for the purpose of marketing.

5.2 A responsible party may only approach a data subject whose consent is required, and who has not previously withheld such consent, once to gain consent and such consent must be in the prescribed manner and form.

6 Accuracy

6.1 A responsible party must take reasonably practical steps to ensure that PI is complete, accurate, not misleading and updated where necessary.

6.2 The PI shall not be updated routinely, unless it is required to fulfill the purpose for which the PI was collected.

7 Safeguards

7.1 A responsible party must secure the integrity and confidentiality of the PI in its possession or under its control by taking appropriate, reasonable technical and organisational measures to prevent loss, damage or unauthorised destruction, unlawful access to, or processing of the PI.

7.2 Anyone processing PI on behalf of a responsible party must:

- treat the information as confidential and not disclose it unless required by law;
- apply the same security measures as the responsible party;
- if domiciled outside the Republic, comply with local protection of personal information laws.

- 7.3 The Data Subject may request responsible party to:
- correct or delete PI that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully;
 - delete or destroy PI that the responsible party is no longer authorised to retain.
- 7.4 The Officer shall ensure that all employees and volunteers know the importance of keeping personal information confidential.
- 7.5 The processing must be governed by a written contract ensuring safeguards are in place.
- 7.6 The Officer shall ensure that care is taken when personal information is disposed of or destroyed to prevent unauthorized parties from gaining access to it.

8 Openness

- 8.1 The Responsible Person must take reasonably practicable steps to ensure the Data Subject is aware of :
- the information being collected;
 - the name and address of the Responsible Party;
 - the purpose for which the information is being collected;
 - whether or not the supply of the information is voluntary or mandatory;
 - the consequences of failure to provide the information;
 - any particular law authorising the requiring of the collection;
 - the right of access to and the right to rectify the information collected;
 - the fact that, where applicable, the responsible party intends to transfer the information to another country/international organisation and the level of protection afforded by that country/organisation; and
 - the right to object to the processing of the information.

This must done prior to collecting PI if the PI is collected directly from the data subject, or in any other case as soon as is reasonably practical after collection.

8.2 Policies and information about the related practices shall be available without unreasonable effort in a format that is generally understandable.

9 Individual Access

9.1 The Officer shall ensure that upon request, Genesis Capital shall inform an individual whether Genesis Capital holds personal information about him/her. If possible, the information's source shall also be given. Genesis Capital shall allow the individual access to the information. Genesis Capital may, however, choose to make sensitive medical information about its employees or volunteers available through a medical practitioner. Genesis Capital shall also account for the use that has been made or is being made of this information and give an account as to the third parties to whom it has been disclosed. (Note, if the Officer believes for valid reasons that access to personal information should be denied, the Officer shall have the right to consult legal counsel before making such a decision.)

9.2 A person requesting his/her personal information may be required by the Officer to give sufficient information to permit Genesis Capital to provide an account of the existence, use, and disclosure of personal information. Information shall be used only for the purpose for which it was obtained.

9.3 If Genesis Capital has supplied personal information about an individual to third parties, the Officer shall ensure that an attempt is made to be as specific as possible. When it is impossible to give a list of organisations to which Genesis Capital has actually disclosed information about an individual, Genesis Capital shall provide a list of organisations to which it might have disclosed information about the individual.

9.4 The Officer shall ensure that GENESIS CAPITAL responds to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be made available in a generally understandable form. For example, the organisation shall explain abbreviations or codes it uses to record information.

9.5 The Officer shall ensure that when an individual successfully demonstrates the inaccuracy or incompleteness of personal information, Genesis Capital shall amend the

information as required. Depending on the information challenged, amendment involves the correction, deletion, or addition of information in question.

- 9.6 The Officer shall ensure that when a challenge is not resolved to the individual's satisfaction, Genesis Capital shall record the unresolved challenge's substance. When appropriate, the unresolved challenge's existence shall be transmitted to third parties having access to the information in question.

REVIEW OF THE PROTECTION OF PERSONAL INFORMATION POLICY

The Protection of Personal Information Policy will be regularly reviewed, internally or by an outside party such as an auditor or compliance officer, and where necessary, updated to ensure that the arrangements remain adequate to identify, assess, evaluate and successfully control Personal Information; the policy will be overseen by the Operations Committee who carry responsibility for the implementation, reviewing and updating process.