PROTECTION OF PERSONAL INFORMATION POLICY

Applicable Risk	Regulatory
Risk Owner	Board of Directors
Recommended by	Information Officer
Approved by	Board of Directors
Effective date	1 June 2021
Review date	31 May 2023

TABLE OF CONTENTS

1. INTRODUCTION

1.1 The Protection of Personal Information Act, 2013 ("POPI") gives effect to the constitutional right of privacy, regulates the manner in which personal information may be processed and provides rights and remedies to protect personal information.

1.2 This policy outlines how the company collects, uses, stores, processes, and shares personal information of its data subjects.

1.3 The types of information that the company may be required to handle include details of current, past and prospective employees, directors, shareholders and clients, suppliers, joint venture partners and other stakeholders of the like that the company communicates with.

1.4 Personal information, whether held on paper or on a computer or other media, is subject to certain legal safeguards specified in POPI which include imposing restrictions on how the company may use that information.

1.5 The policy applies to all:

1.5.1 personal information collected, used, transformed or produced by the company;

1.5.2 employees of the company in so far as they are involved in the processing of personal information; and

1.5.3 service providers, contractors and other third parties who have access to personal information in the company's control and/or possession;

1.6 Objective and purpose of this policy

1.6.1 This policy sets out the company's rules on personal information protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

1.6.2 The purpose of the policy is to establish management direction and high-level objectives for regulating the manner in which personal information is processed and to provide for remedies in cases where personal information is not handled accordingly.

1.6.3 Further purposes of the policy include:

i) compliance with the requirements of POPI;

ii) providing a unified policy regarding the methods and procedures for the retention and destruction of documents;

iii) ensuring records that are no longer required or documents that are of no value are destroyed properly and in accordance with the provision herein; and

iv) providing assistance to employees in understanding the requirements relating to the protection of personal information and the retention and destruction of documents.

2. DEFINITIONS

2.1 “appeal forum” means a forum made up of the company’s compliance officer, key individual and a director constituted for the purpose considering appeals to complaints lodged by data subjects or any other persons;

2.2 “automated decision” means a decision that is made when personal information is analysed to make a decision without human intervention in that decision-making process;

2.3 “company” means Empowerment Capital Investment Partners (Pty) Ltd;

2.4 “consent” means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information;

2.5 “data subject” means the person to whom personal information relates;

2.6 “direct marketing” means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:

2.6.1 promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or

2.6.2 requesting the data subject to make a donation of any kind for any reason;

2.7 “electronic communication” means any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient’s terminal equipment until it is collected by the recipient;

2.8 “employee(s)” means persons in the employ of the company;

2.9 “Information Officer” means an employee who has been appointed as the company’s information officer;

2.10 “Information Regulator” means the information regulator established in terms of section 39 of POPI;

2.11 “operator” means a person who processes personal information for the company as a responsible party in terms of a contract or mandate, without coming under the direct authority of the company;

2.12 “personal information” means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to:

2.12.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

2.12.2 information relating to the education or the medical, financial, criminal or employment history of the person;

2.12.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

2.12.4 the biometric information of the person;

2.12.5 the personal opinions, views or preferences of the person;

2.12.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

2.12.7 the views or opinions of another individual about the person; and

2.12.8 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;

2.13 “POPI” means the Protection of Personal Information Act 4 of 2013 together with regulations thereunder from time to time;

2.14 “processing” means any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including:

2.14.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; or

2.14.2 dissemination by means of transmission, distribution or making available in any other form; or

2.14.3 merging, linking, as well as restriction, degradation, erasure or destruction of information;

2.15 “processor” means an employee of the company whose work involves the use and processing of personal information;

2.16 “records” shall have the meaning ascribed to it in POPI;

2.17 “responsible party” means the company, as a private body which, alone or in conjunction with any other person determines the purpose of and means for processing personal information; and

2.18 “special personal information” means personal information, the religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

3. PROCESSING CONDITIONS

The company must comply with the following eight conditions for the lawful processing of personal information as prescribed by POPI:

3.1 Accountability: A responsible party must comply with all the conditions for lawful processing.

3.2 Purpose specification: Personal information must only be collected for a specific, explicitly defined lawful purpose related to a function or activity of the responsible party.

3.3 Processing limitation: Processing must be justified on a ground recognized under POPI, for example, consent/legitimate interests of the data subject, responsible party or the third party to whom the information is supplied.

3.4 Further processing limitation: Processing must be in accordance with or compatible with the purpose for which it was initially collected subject to limited exceptions.

3.5 Information quality: Steps must be taken to ensure that the information is complete, accurate, not misleading and updated where necessary.

3.6 Openness: Notification requirements must be complied with when collecting personal information.

3.7 Security safeguards: Appropriate, reasonable technical and organizational measures must be implemented and maintained to prevent loss of, damage to or unauthorized destruction of or unlawful access to personal information.

3.8 Data subject participation: data subjects have the right to request details of the personal information that a responsible party holds about them and, in certain circumstances, request access to such information.

4. RESPONSIBILITY AND ACCOUNTABILITY

4.1 The company must ensure that the conditions for the lawful processing are complied with.

4.2 The Chief Executive Officer of the company is the appointed Information Officer.

4.3 The Information Officer is appointed to encourage and support the company's overall compliance with POPI, including:

4.3.1 taking responsibility for drafting policies and procedures, which will, among other things, address the company's compliance with POPI;

4.3.2 designating specific individuals to monitor compliance with POPI; and

4.3.3 undertaking training awareness sessions for employees on POPI.

4.4 The Information Officer is responsible for administering and overseeing the implementation of this policy.

4.5 Processors shall be accountable to the Information Officer.

4.6 The collection, use and retention of personal information must be effected only with the Information Officer's written consent or delegation.

4.7 Any employee or a data subject suspecting that personal information is being used for purposes other than that explicitly collected for, may register a complaint with the Information Officer.

4.8 The Information Officer shall investigate the above complaint and inform the complainant of his or her findings and corrective action taken.

4.9 If the complainant is dissatisfied with the findings of the Information Officer, an appeal may be submitted to the appeal forum and thereafter the determination made by the appeal forum will be final.

5. PURPOSE OF COLLECTION OF PERSONAL INFORMATION

5.1 Personal information must be collected for a specific, explicitly defined and lawful purpose related to the function or activity of the company.

5.2 The data subject must be made aware of the purpose of the collection.

6. SECURITY

6.1 The company must keep all personal information secure against the risk of loss, unauthorised access, interference, modification, destruction or disclosure and conduct regular risk assessments to identify and manage all reasonably foreseeable internal and external risks to personal information under its control.

6.2 The company may engage with other organisations to provide support services for the security of company information. Third parties are obliged to comply with the confidentiality requirements of any personal information held by the company. Service Level Agreements with third parties will include a data protection clause in order to ensure adherence with the company’s data protection requirements.

6.3 All employment contracts must include a confidentiality clause and/or data protection clause.

6.4 The company will not disclose any personal information to third party unless:

6.4.1 it is compelled to comply with legal and/or Information Regulatory requirements or when it is otherwise allowed by law;

6.4.2 it is in the public interest; or

6.4.3 the company needs to do so to protect its rights.

6.5 The company must not retain records any longer than is necessary for achieving the purpose for which it was collected unless:

6.5.1 further retention is required by law;

6.5.2 the company reasonably requires to keep it;

6.5.3 retention is required by a contract between the parties;

6.5.4 the data subject consents to the further retention.

6.6 Personal information 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.

6.7 Provisions with operators:

6.7.1 operators include call centres, outsourced payroll administrators, marketing database companies, recruitment agencies, psychometric assessment centres, document management warehouses, external consultants and credit bureaus.

6.7.2 the company will implement the following key obligations in respect of operators:

i) the operator may not process personal information on behalf of the company without the knowledge and authorisation of the company;

ii) the company will ensure that the operator implements the security measures required;

iii) there will be a written contract in place between the company and the operator which requires the operator to maintain the confidentiality and integrity of personal information processed on behalf of the company;

iv) the written contract between the company and the operator will include the provisions set out in Annexure A hereto; and

v) if the third party is located outside of South Africa, the company will consult the Information Officer.

7. CONSENT

7.1 When collecting personal information, the company shall obtain voluntary, informed and specific consent from the data subject, to use, collect, retain or disclose said personal information.

7.2 Consent must be obtained before collecting personal information.

7.3 When collecting personal information, the company shall ensure that the data subject understands how the personal information will be used.

7.4 Express consent will be obtained from the data subject, unless in the Information Officer's opinion implied consent will be acceptable. The consent must be clear and verifiable.

7.5 The reasonable expectations of the data subject will be respected.

7.6 A data subject may (i) withdraw its consent at any time and such withdrawal of consent should be noted and (ii) may also object at any time on reasonable grounds, to the processing of its personal information, save if other legislation provides for such processing.

7.7 Upon the data subject withdrawing its consent, the company may no longer process its personal information.

8. PURPOSE SPECIFICATION

8.1 Personal information may only be processed for specific, explicitly defined and legitimate reasons relating to the functions or activities of the company, of which the data subject is made aware.

8.2 Personal information will only be collected to the extent that it is required for the specific purpose notified to the data subject.

8.3 Any personal information which is not necessary for a specified purpose will not be collected in the first place.

8.4 Once collected, personal information must only be processed for the specific purposes notified to the data subject when the personal information was first collected or for any other purposes specifically

permitted by POPI. This means that personal information may not be collected for one purpose and then used for another.

8.5 If it becomes necessary to change the purpose for which personal information is processed, the data subject will be informed of the new purpose before any processing occurs.

8.6 Records of personal information may only be kept for as long as necessary for achieving the purpose for which the information was collected or subsequently processed, unless:

8.6.1 retention of the record is required or authorised by law;

8.6.2 the company reasonably requires the record for lawful purposes related to its functions or activities;

8.6.3 retention of the record is required by a contract between the parties thereto; or

8.6.4 the data subject or a competent person where the data subject is a child has consented to the retention of the record.

8.7 Personal information will therefore not be kept longer than is necessary for the purpose for which it was collected and must therefore be destroyed or deleted in a manner that prevents its reconstruction in an intelligible form or be deidentified as soon as reasonably practicable after the company is no longer authorised to retain the record. For guidance on how long certain personal information will be kept before being destroyed, see the company's Records Management Policy.

8.8 The company may process a data subject's special personal information in any one of the following circumstances:

8.8.1 if data subject has consented to the processing; or

8.8.2 if the processing is needed to create, use or protect a right or obligation in law; or

8.8.3 if the processing is for statistical or research purposes and all legal conditions are met; or

8.8.4 if the special personal information was made public by the data subject; or

8.8.5 if the processing is required by law; or

8.8.6 if demographic information is processed, and the processing is required to identify the data subject.

9. LIMITING COLLECTION AND FURTHER PROCESSING

9.1 The company is an authorised financial services provider in terms of the Financial Advisory and Intermediary Services Act 37 of 2002 (FAIS), and an accountable institution, in terms of the Financial Intelligence Centre Act (FICA).

9.2 Through the services it renders in terms of FAIS and the client due diligence information it is required to collect in terms of FICA, the company is necessarily involved in collecting, using and disclosing certain aspects of the personal information of its clients, employees and other stakeholders.

9.3 Personal information must be collected directly from a data subject except:

9.3.1 if the information is contained in a public record or has deliberately been made public by the data subject; or

9.3.2 if the data subject has consented to the collection from another source; or

9.3.3 if collection from another source would not prejudice a legitimate interest of the data subject; or

9.3.4 if collection from another source is necessary to maintain law and order; or

9.3.5 to enforce legislation concerning the collection of revenue; or

9.3.6 for the conduct of court or tribunal proceedings; or

9.3.7 in the interests of national security; or

9.3.8 if compliance would prejudice a lawful purpose of the collection; or

9.3.9 if compliance is not reasonably practicable in the circumstances of the particular case.

9.4 Further processing must be compatible with the purpose for which it was collected, unless the data subject gives consent to the further processing.

9.5 Where personal information is transferred to a third party for further processing, the further processing must be compatible with the purpose for which it was initially collected.

9.6 If personal information is to be used for any other purpose the further consent of the data subject must be obtained. Where this is not possible, the Information Officer should be consulted.

9.7 The company may use a data subject's personal information to make an automated decision as allowed by the law, for example, the approval or decline of an investment. A data subject has a right to query any such decisions made and will be provided reasons for the decisions as far as reasonably possible.

9.8 The company may obtain personal information from credit bureau for any of the following reasons:

9.8.1 if a data subject has requested the company to do so or has so consented; or

9.8.2 to verify (check and confirm) a data subject's identity; or

9.8.3 to obtain or verify a data subject's employment details; or

9.8.4 to obtain, verify or update a data subject's contact or address details; or

9.8.5 to obtain a credit report about a data subject (which includes a data subject's credit history and credit score) when they apply for a credit agreement; or

9.8.6 to determine a data subject's credit risk; or

9.8.7 for debt recovery purposes; or

9.8.8 to trace the whereabouts of a data subject; or

9.8.9 to update a data subject's contact details; or

9.8.10 to build credit scorecards which are used to evaluate transaction applications.

9.9 The company will share a data subject's personal information with *inter alia* the BEE Commission, the Financial Sector Conduct Authority, a BEE verification Agency, the Board of Directors of Subsidiary companies to, among others, report:

9.9.1 an application for a transaction agreement; or
9.9.2 the opening of a transaction agreement; or

9.9.3 the termination of a transaction agreement; or

9.9.4 payment behaviour on a transaction agreement; or

9.9.5 non-compliance with a transaction agreement, such as not paying in full or on time.

10. ACCURACY

10.1 The company must take reasonably practical steps to ensure that personal information is complete, accurate, not misleading and updated where necessary.

10.2 Information which is inconsistent or misleading is not accurate and steps must therefore be taken to check the accuracy of any personal information at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date information will be destroyed.

10.3 Personal information need not be updated routinely, unless it is required to fulfil the purpose for which it was collected.

10.4 The Information Officer must develop processes for:

10.4.1 checking the accuracy and completeness of records containing personal information;

10.4.2 dealing with complaints relating to the timeliness and accuracy of personal information;

10.4.3 data subjects to periodically verify and update their personal information;

10.4.4 making data subjects aware of these processes; and

10.4.5 monitoring and tracking updates to personal information.

10.5 The Information Officer will furthermore put procedures in place to verify that records containing personal information remain relevant, accurate and up-to date.

11. OPENESS

Prior to collecting personal information either directly from the data subject or in any other case as soon as is reasonably practical after collection, employees must take reasonably practicable steps to ensure that data subject is aware of:

11.1 The information being collected and where the information is not directly collected from the data subject, the source from which it is collected.

11.2 The name and address of the company.

11.3 The purpose for which the information is being collected.

11.4 Whether or not the supply of information is voluntary or mandatory.

11.5 The consequences of failure to provide the information.

11.6 Any particular law authorising the requiring of the collection.

11.7 The right of access to and the right to rectify the information collected.

11.8 The fact that, where applicable, the company intends to transfer the information to another country or an international organisation and the level of protection afforded by that other country or international organisation.

11.9 The right to object to the processing of the information.

11.10 The right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator.

12. DATA SUBJECT ACCESS

12.1 The company recognizes that a data subject has the right to have the company confirm, free of charge, whether or not it holds personal information about the data subject and may request the company to provide a record or a description of the personal information held, including information about the identity of all third parties, or categories of third parties, who have, or have had, access to the information at a prescribed fee.

12.2 The Information Officer shall ensure that upon request, the company shall inform the data subject whether the company holds personal information about that data subject. If possible, the source of the information shall also be given. The company shall allow the data subject access to the information.

12.3 The data subject requesting access to personal information may be required by the Information Officer to give sufficient information to permit the company to provide an account of the existence, use and disclosure of personal information.

12.4 If the company has supplied personal information about a data subject to
third parties, the Information Officer shall ensure than an attempt is made to be as specific as possible.

12.5 The Information Officer shall ensure that the company responds to a data subject's request within a reasonable time and at a minimum or no cost to the data subject. The requested information shall be made available in generally understandable form.

12.6 A request to correct or delete personal information will be processed in line with a data subject’s right to request the company to:

12.6.1 provide access to any personal information held about them; or

12.6.2 prevent the processing of their personal information for purposes of direct marketing; or

12.6.3 have inaccurate personal information amended if it is inaccurate, irrelevant, excessive, misleading or obtained unlawfully; or

12.6.4 have personal information destroyed or deleted if the company is no longer authorised to retain; or

12.6.5 object to any decision that significantly affects them being taken solely by a computer or other automated process.

12.7 The Information Officer shall ensure that when a data subject correctly demonstrates the inaccuracy or incompleteness of personal information, the company shall amend the information as required.

12.8 The company will provide credible proof to a data subject of the action that has been taken in response to the request.

12.9 The Information Officer shall ensure that when a challenge is not resolved to the data subject's satisfaction, the company shall record the grounds of such challenge. When appropriate, the unresolved challenge's existence shall be transmitted to third parties having access to the information in question.

12.10 If any changes to the personal information will have an impact on any decisions to be made about a data subject, the company will inform all third parties to whom the information has been disclosed, including any credit bureaus, of such changes

13. SHARING OF PERSONAL INFORMATION

13.1 Employees dealing with enquiries from third parties should be careful about disclosing any personal information held by the company. In particular they should:

13.1.1 check the identity of the person making the enquiry and whether they are legally entitled to receive the information they are requesting;

13.1.2 suggest that the third party puts their request in writing so the third party's identity and entitlement to the information may be verified;

13.1.3 refer to the Information Officer for assistance in difficult situations; and

13.1.4 where providing information to a third party, do so in accordance with the processing conditions.

13.2 Current employees will be required to sign an addendum to their employment contracts containing relevant consent clauses for the use and storage of employee information, or any other action so required, in terms of POPI.

14. FAIR AND LAWFUL PROCESSING

14.1 POPI is aimed at ensuring that the processing of personal information is done fairly and without adversely affecting the rights of the data subject.

14.2 For personal information to be processed lawfully, certain requirements have to be met, including (i) obtaining a data subject’s consent to the processing, or (ii) the processing is necessary for the legitimate interest of the company or the party to whom the personal information is disclosed.

14.3 When special personal information is being processed, a data subject's explicit consent to the processing of such information will be required.

14.4 Personal information about employees may be processed for legal, personnel, administrative and management purposes and to enable the company to meet its legal obligations as an employer, for example, to pay employees, monitor their performance and to confer benefits in connection with their employment.

14.5 For examples, special personal information of employees is likely to be processed for the following reasons:

14.5.1 information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;

14.5.2 the employee's racial or ethnic origin or religious or similar information in order to monitor compliance with employment equity legislation; and

14.5.3 in order to comply with legal requirements and obligations to third parties.

15. ELECTRONIC AND DIRECT MARKETING

15.1 The Electronic Communications and Transactions Act, 2002 (ECTA) and the Consumer Protection Act, 2008 empower consumers to restrict unwanted direct marketing. Under these laws, a data subject must be given the opportunity to opt out of receiving marketing information, free of charge.

15.2 Unless a data subject has given its consent, or the email recipient is an existing client of the company, the processing of a data subject's personal information for the purposes of direct marketing by means of unsolicited electronic communications is prohibited.

15.3 The company may only approach a data subject once in order for the data subject to opt in to receive marketing information.

15.4 When sending emails to a data subject who is an existing client:

15.4.1 the company must have obtained the details of the data subject through a sale of a product or service;

15.4.2 the marketing should relate to similar products or services of the company; and

15.4.3 the data subject must have been given a reasonable opportunity to unsubscribe or “opt- out”, free of charge, of the use of its personal information for direct marketing purposes.

15.5 All direct marketing communications must contain an “unsubscribe” option.

15.6 Any communication for the purpose of direct marketing must contain the details of the identity of the sender or the person on whose behalf the communication has been sent and an address or other contact details to which the recipient may send an instruction to “opt-out” or unsubscribe.

15.7 No direct marketing communication may be sent during the following times: Sundays or public holidays; Saturdays before 09h00 and after 13h00; and all other days between the hours of 20h00 and 08h00 the following day, except to the extent that the data subject has agreed otherwise.

16. TRANSFER

16.1 There are two instances relating to the transfer of personal information, namely, where a person in South Africa sends personal information to another country to be processed and where a person in South Africa processes personal information that has been received from outside South Africa.

16.2 The requirements for the processing of personal information prescribed in POPI will apply to any personal information processed in South Africa, irrespective of its origin.

16.3 The company will not transfer personal information to a third party in another country unless:

16.3.1 the recipient is subject to laws, binding corporate rules or a binding agreement which upholds principles for reasonable processing of the information that are substantially similar to the conditions contained in POPI and include provisions that are substantially similar to those contained in POPI relating to the further transfer of personal information from the recipient to third parties who are in another country; or

16.3.2 the data subject consents to the transfer; or

16.3.3 the transfer is necessary for the performance of a contract between the data subject and responsible party, or for the implementation of pre-contractual measures taken in response to the data subject’s request; or

16.3.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of a data subject between the responsible party and a third party, or the transfer is for the benefit of the data subject; or

16.3.5 it is not reasonably practicable to obtain the consent of the data subject to that transfer, and if it were reasonably practicable to obtain such consent, the data subject would be likely to give it.

17. BREACH OF POLICIES

A breach of this policy and/or any other policy or policies and procedures put in place as a result of this policy, the POPI Compliance Framework, including a breach of the company's Information Security Management Policy, Data Breach Notification Policy, Records Management Policy and the POPI Manual, will result in disciplinary proceeding which may lead to dismissal.